DIAGNÓSTICO Y PLAN DE ACCIÓN PARA LA IMPLEMENTACIÓN DE PCI EN LA OPERACIÓN METLIFE DE LA COMPAÑÍA INTERCONTACT

DAMIAN ORLANDO COLORADO GUARNIZO
SANLY APONTE GÓMEZ

UNIVERSIDAD PILOTO DE COLOMBIA
POSGRADO EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2017

DIAGNÓSTICO Y PLAN DE ACCIÓN PARA LA IMPLEMENTACIÓN DE PCI EN LA OPERACIÓN METLIFE DE LA COMPAÑÍA INTERCONTACT

DAMIAN ORLANDO COLORADO GUARNIZO
SANLY APONTE GÓMEZ

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor
ING. ÁLVARO ESCOBAR ESCOBAR

UNIVERSIDAD PILOTO DE COLOMBIA
POSGRADO EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2017

AUTORIDADES ACADÉMICAS

DRA. PATRICIA PIEDRAHITA CASTILLO

Rectora

DRA. SANDRA XIMENA FARFAN

Directora Posgrado

ING. ÁLVARO ESCOBAR ESCOBAR

Director Especialización Seguridad en Informática

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

Firma Presidente del Jurado

Firma Jurado

Firma Jurado

Bogotá, Julio de 2017

AGRADECIMIENTOS

Agradecemos a Intercontac S.A.S por su colaboración en el diagnóstico y plan de acción para la implementación de PCI en la operación Metlife de su compañía.

Gracias a Ing. Jenny Alejandra Varela Segura y Ing. Álvaro Escobar Escobar, y demás ingenieros que fueron parte fundamental en el direccionamiento para alcanzar los objetivos planteados en el diagnóstico y plan de acción para la implementación de PCI.

Las asesorías permitieron dirigir los conocimientos obtenidos a través de la especialización y así aportar un proceso confiable en el desarrollo del proyecto.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICAS

Pág.

RESUMEN

Intercontact es una compañía fundada en el año 2009 que presta servicios de contact center, dentro de sus clientes esta la compañía Metlife cuya relación comercial consta en el uso de Intercontact para la venta de seguros de vida por medio de contacto telefónico y recolección de datos por medio de una aplicación Web. Esta venta de seguros involucra el almacenamiento, tratamiento y trasferencia de datos del titular de la tarjeta y en la actualidad los procedimientos establecidos para ejecutar estas tareas, no cumplen con regulaciones interpuestas por las compañías de tarjetas débito y crédito.

Con el fin de evitar los fraudes que involucran el manejo de datos de tarjetas de pago débito y crédito, arriesgar la pérdida de sus permisos para procesar estos datos y evitar pago de multas, Intercontact ha decidido implementar la PCI DSS.

Para ello se debe establecer las pautas que Intercontact debe tener en cuenta para poder implementar la norma, realizando un análisis GAP con el fin de determinar cuál es el estado actual y el estado deseado relacionado con el cumplimiento de la norma PCI DSS en la campaña Metlife tomando como base una metodología CMMI.

Luego de realizar el análisis GAP es necesario establecer varios planes de acción que logren llegar a un estado Definido con relación a los controles de la norma PCI-DSS, esto quiere decir que el control está documentado, se ha divulgado, pero no se realizan mediciones de su desempeño. De acuerdo a esto la compañía empezaría a realizar otras mejoras para Madurar en la implementación y cumplimiento de la PCI-CSS en la campaña Metlife.

En paralelo se sugiere el orden, tiempo y responsables necesarios para ejecutar esta serie de actividades con un cronograma que debe ser desarrollado o ejecutado a lo largo de un periodo aproximado de año y medio, en el cual se establece como fecha de inicio de ejecución de actividades el 01 de Septiembre del 2017 y una fecha de finalización del 03 de mayo del 2019.

Luego de todas estas actividades Intercontact podría estar listo realizar la autoevaluación utilizando un cuestionario provisto por el Consorcio del PCI (PCI SSC) demostrando el cumplimiento de la norma.

Palabras Claves: Seguridad informática, Norma PCI, tarjetas de pago y DMZ (Demilitarized Zone).

ABSTRACT

Intercontact is a company that was founded in the 2009, which provides contact center services; among its clients is the MetLife Company. This relationship consists of the use of Intercontact to sell life insurance through telephone contact and data collection by means of a Web application. The sale of insurance services involves the storage, treatment and transfer of data of the cardholder and currently these established procedures to perform these tasks do not comply with regulations brought by credit card and debit card companies.

In order to avoid scams and fraud that involve the handling of data of credit and debit card payments, risk the loss of their permits to process these data and avoid fines, Intercontact has decided to implement the PCI DSS.

To do this, guidelines must be set that Intercontact must take into account in order to implement the standard/norm. By performing, a GAP analysis to determine what is the current state and the desired state related to compliance with the PCI DSS standard in the MetLife campaign based on a CMMI methodology.

After performing the GAP analysis, it is necessary to establish several action plans to reach a defined state relative to the PCI-DSS standard controls, this means that the control is documented, has been reported, but their performance measurements are not carried out. According to this the company would begin to make other improvements to advance and reach the implementation and compliance of the PCI-CSS in the MetLife campaign.

At the same time, it is suggested that, time, order and responsible parties needed to run this series of activities. This should be done with a timetable/schedulle that should be developed or executed over an approximate period of a year and a half, which sets as a start date for implementation of activities on 01 September 2017 and finish May 03 of 2019.

After all these activities Intercontact could be ready to perform the self-evaluation using a questionnaire provided by the consortium of the PCI (PCI SSC) demonstrating compliance with the standard/norm.

Keywords: Informatic security, PCI standard, payment cards,Gap analysis y CMMI methodology

1. INTRODUCCIÓN

El procesamiento, almacenamiento, transferencia y manejo de información son un tema de preocupación para todas las organizaciones y compañías en general, las implicaciones legales, regulatorias, pérdidas económicas, de reputación e imagen que pueden incurrir en una compañía puede llevarla a la quiebra.

Garantizar el debido tratamiento de la información en aspectos como confidencialidad, integridad y disponibilidad de la información son vitales en cualquier organización que maneje o trate cualquier tipo de información.

En la actualidad, existen varias metodologías que pueden ayudar a una organización a llevar a cabo un debido y acertado manejo para manipular y tratar la información de manera segura, entre estas metodologías está presente la norma ISO27001.

En muchas organizaciones que manipulan información con un grado de sensibilidad mayor como es el caso de datos de tarjetas de crédito, débito y datos del titular, normas como la ISO27001 quedan cortas o su alcance no es suficientemente específico y profundo en temas puntuales, es necesario apoyarse en estándares que cobijen o guíen de manera adecuada la debida manipulación de esta información de manera segura.

El estándar PCI DSS ofrece controles que garantizan el almacenamiento, procesamiento y transporte seguro de la información de tarjetas de pago y datos del titular, en el caso de la compañía Intercontact cuenta con una operación llamada Metlife que manipula este tipo de información en sus pagos de seguros de vida.

Por esta razón nace la necesidad que Intercontact aplique un estándar modelo que garantice el cumplimiento necesario de seguridad en la manipulación de datos de tarjetas de pago y del titular.

2. JUSTIFICACIÓN

Intercontact es una compañía de Contact Center que presta sus servicios de venta de seguros a la empresa Metlife cuyo fin es ofrecer seguros de vida y de otro tipo de seguros a personal afiliado a diferentes cajas de compensación familiar. Estos seguros son vendidos por medio de descuentos realizados a la tarjeta de compensación familiar, pero en caso de que el potencial cliente no cuente con esta tarjeta, este seguro puede ser descontado de su tarjeta de crédito en cuotas mensuales o descontadas directamente de su tarjeta de débito en un pago semestral o anual.

Cuando el usuario ha dado el visto bueno para adquirir su seguro, los datos del titular y los diferentes datos de las tarjetas de pago son enviadas a la empresa Metlife para que este realice el debido descuento.

El procedimiento que involucran la manipulación de estos datos de tarjetas de pago y datos del titular cuya actividades evidencian la manipulación inadecuada de las mismas como son la gestión de las llamadas, la recolección de datos, aplicaciones en las cuales los datos son consignados, los perfiles de usuarios en los aplicativos de los clientes o terceros, control de acceso, generación de reportes, manipulación de grabaciones, almacenamiento y disposición de estas, la comunicación con el cliente y demás aspectos relevantes que muestran falencias con los requerimientos mínimos que debe tener una organización que procese, gestione, almacene o transmita datos de tarjetas de crédito, débito y datos del titular, es necesario basarse en un estándar que aplique e identifique controles que deben ser implementados para mitigar estas falencias.

El estándar de seguridad de datos de la industria de tarjetas de pago (PCI-DSS) ha desarrollado controles y actividades en busca de mejorar la seguridad de los datos del titular y de las tarjetas de pago y se aplica para empresas que almacenan o transmiten CHD (datos del titular de la tarjeta) y datos de la tarjeta, como es en el caso Intercontact en su operación de venta de seguros de Metlife.

Por esta razón para dar cumplimiento a requerimientos legales, de clientes y demás partes interesadas debería realizar todas con la implementación de los controles y actividades estipuladas por el estándar PCI, dada que esta cumple con todos los componentes del sistema incluidos en el entorno de datos del titular de la tarjeta o los conectados a este, con el fin de mitigar riesgos y dar cumplimiento con la estrategia empresarial de Intercontact.

Implementar los controles y buenas prácticas generadas por el estándar PCI ofrece ventajas a nivel competitivo y de valor agregado ante otras empresas del mismo sector del mercado de igual manera que da cumplimiento al tratamiento de datos de acuerdo a leyes y regulaciones impuestas.

El cumplimiento de la Norma ISO27001 no cubre todos los aspectos necesarios para garantizar el uso adecuado de los datos de tarjetas de pago y datos del titular, se deben implementar controles más específicos y fuertes que puedan garantizar ciertos aspectos en seguridad. Si la empresa desea ampliar su ventaja competitiva ante otras empresas del sector de negocio y ofrecer sus servicios a compañías reconocidas del sector financiero, seguros, comercio y servicios quienes exigen el debido cumplimiento de este estándar a sus proveedores cuya función es de almacenar, transmitir o gestionar datos de sus clientes, es necesario que Intercontact implemente y se certifique en un estándar internacional como es PCI-DSS.

Asi mismo, Intercontact se beneficia en aspectos como es la protección de la compañía de posibles pérdidas de ingresos, investigaciones no deseadas y costos legales, prevenir la fuga y robo de información, entre otros.

3. PROBLEMA

3.1 PLANTEAMIENTO DEL PROBLEMA

La compañía Intercontact es un Contact Center cuya misión es: “Posicionar a INTERCONTACT S.A.S. como compañía prestadora de servicios integrales confiables, productivos de alto valor tecnológico y flexible ante las necesidades de sus clientes”[1]; en la actualidad presenta un problema con la gestión indebida e insegura en el procesamiento, almacenamiento y transmisión de datos de tarjetas de crédito, débito e información del titular de la tarjeta. En los cuales se destacan actividades como la mala manipulación de grabaciones, aplicaciones inseguras, transporte inapropiado de información, controles de acceso débiles, roles y permisos sin gestión, análisis de vulnerabilidades en lapsos muy largos, datos del titular de la tarjeta sin la debida protección, desarrollo de aplicaciones que no usa los parámetros de seguridad necesarios, no se realiza supervisión ni rastreo de los accesos a los recursos de red y a los datos del titular de la tarjeta, zonas DMZ con configuraciones a nivel de seguridad bajas, falta de documentación relacionada a configuración de políticas y parámetros en el *firewall*, bajos niveles de seguridad en dispositivos móviles corporativos, falta de capacitación en temas específicos relacionados al uso adecuado de datos sensibles, no existe *hardening* en los servidores, políticas de retención de datos ineficientes, no se cumple con un procedimiento de gestión de cambios a nivel de desarrollo eficiente, comunicaciones inseguras, registros de auditoria insuficientes, no se realizan pruebas de penetración entre otras.

Por requerimientos contractuales, legales y de cumplimiento ante clientes y entidades se debe gestionar estos aspectos; generando e implementando los debidos controles y actividades que son necesarios para dar cumplimiento a las necesidades y expectativas de las partes interesadas. Y así ejecutar los requisitos mínimos en seguridad que se deben tener cuando una entidad procese, transmite o almacene datos de tarjetas de crédito o del titular de la misma; seleccionando un modelo de gestión e implementación de los controles.

3.2 PREGUNTA PROBLEMA

¿De qué forma la compañía Intercontact SAS gestionara y procesara de manera adecuada y segura los datos de tarjetas de crédito, débito y datos del titular para la operación Metlife en su sede principal de Bogotá?

[1] INTERCONTACT CENTER, 2017

4. TÍTULO

DIAGNÓSTICO Y PLAN DE ACCIÓN PARA LA IMPLEMENTACIÓN DE PCI EN LA OPERACIÓN METLIFE DE LA COMPAÑÍA INTERCONTACT.

5. OBJETIVOS

5.1 GENERAL

Realizar un diagnóstico y plan de acción para dar cumplimiento a los requerimientos mínimos necesarios para procesar, trasmitir y almacenar datos de tarjetas de pago y titular, teniendo como base los controles exigidos por el estándar PCI DSS para la empresa Intercontact en su operación Metlife.

5.2 OBJETIVOS ESPECÍFICOS

- Realizar un Análisis GAP que permita identificar la brecha existente entre las actividades que realiza Intercontact actualmente en el procesamiento, transporte y almacenamiento de información de tarjetas de pago y titular y los requerimientos exigidos por el estándar PCI DSS.
- Definir un plan de acción con las recomendaciones de seguridad necesarias en la compañía Intercontact para cumplir los requerimientos de PCI DSS.
- Generar cronograma para la implementación de tareas y controles para dar solución adecuada a los planes de acción.

6. TIPO DE INVESTIGACIÓN

Estudios descriptivos.

7. HIPÓTESIS

7.1 HIPÓTESIS DE INVESTIGACIÓN

El realizar un Análisis GAP de la operación Metlife y un plan de acción de los no cumplimientos identificados basados en el estándar PCI-DSS, generará un adecuado diagnóstico y diseño con el cual Intercontact pueda gestionar y procesar de manera adecuada y segura los datos de tarjetas de crédito, débito y datos del titular para la operación.

7.2 HIPÓTESIS NULA

El realizar un Análisis GAP de la operación Metlife y un plan de acción de los no cumplimientos identificados basados en el estándar PCI-DSS, no permitirá generar un adecuado diagnóstico y diseño con el cual Intercontact pueda gestionar y procesar de manera adecuada y segura los datos de tarjetas de crédito, débito y datos del titular para la operación.

8. VARIABLES

8.1 VARIABLES INDEPENDIENTES

- Análisis GAP. Requerimientos PCI-DSS.

8.2 VARIABLES DEPENDIENTE

- Diagnóstico.
- Acciones o actividades a realizar.

9. MARCO TEÓRICO

9.1 PCI (*Payment Card Industry Security Standards*)

El estándar PCI consiste en fomentar una serie de buenas prácticas y un conjunto de requisitos mínimos para proteger los datos que pertenecen al titular de la tarjeta de pago, cuyas medidas son cobijadas y aplicadas a nivel mundial.

El estándar PCI-DSS se aplica a todas las entidades que participan en el procesamiento de tarjetas de pago, en el caso de la compañía Intercontact, este estándar aplica debido a que la operación Metlife, almacena, procesa y gestiona, o transmite CDH (datos del titular de la tarjeta) como los datos de la tarjeta aunque no realice directamente la transacción o descuento respectivos a la cuenta.

El estándar PCI-DSS cuenta con 12 principales requisitos. Ver cuadro 1.

Cuadro 1. Descripción general de Alto Nivel

Descripción general	Requisitos pci dss
Desarrolle y Mantenga redes y sistemas seguros.	1. Instalar y mantener una configuración del *firewall* para proteger los datos del titular de la tarjeta.
	2. No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
Proteger los datos del titular de la tarjeta.	3. Proteja los datos del titular de la tarjeta que fueron almacenados.
	4. Cifrar la trasmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad.	5. Utilizar y actualizar con regularidad los programas o *software* antivirus.
	6. Desarrolle y mantenga sistemas y aplicaciones seguras.
Implementar medidas sólidas de control de acceso.	7. Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

Cuadro 1. (Continuación)

Descripción general	Requisitos pci dss
	8. Identifique y autentique el acceso a los componentes del sistema.
	9. Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad.	10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.
	11. Pruebe con regularidad los sistemas y procesos de seguridad.
Mantener una política de seguridad de la información.	12. Mantenga una política que aborde la seguridad de la información para todo el personal.
Fuente: Norma de seguridad de datos de la PCI (Industria de tarjetas de pago), versión 3.0. 2013	

Todos los requisitos de seguridad del estándar PCI-DSS es aplicado a todos los componentes del sistema como los servidores, dispositivos de red, aplicaciones, dispositivos que ofrecen servicios de seguridad y componentes de virtualización en los cuales también está incluido el entorno de los datos del titular de la tarjeta o los que estén conectados a este. Este entorno lo integran los procesos, tecnología, personas que transmiten, procesan y almacenan los datos de titulares de las tarjetas o los datos confidenciales de autenticación.

El estándar PCI-DSS sugiere implementar ciertos controles o actividades que no son requisitos del estándar pero con estos se pueden mitigar ciertos parámetros como son el alcance, evaluación, costo y la dificultad de la implementación del PCI-DSS como es la segmentación de red.

Implementar el estándar PCI-DSS genera varios beneficios para la compañía Intercontact en los cuales se cuenta con promover la integridad del comercio, incrementar las ventas, proteger al comercio de posibles pérdidas de ingresos, reducir el riesgos de compromiso o fuga de información de clientes y derivados de pérdidas financieras, lucha contra la suplantación y otros fraudes, prevenir el robo masivo de información de clientes, facilitar la adopción de estándares de seguridad válidos a nivel mundial, generar una herramienta que establece las posibles

vulnerabilidades que tiene el sistema de información.

Hay que aclarar que quien exige el cumplimiento de PCI son las entidades financieras como VISA, y no el PCI Council que es solo un organismo regulador. Este estándar ha sido creado por las principales marcas de tarjetas como son MasterCard, Visa, American Express, JCB y Discover Financial Services, por esta razón el incumplimiento con el PCI puede conllevar sanciones por parte de las principales marcar de tarjetas. Se han establecido diferentes niveles de clasificación para los comercios y proveedores de servicios, y estas implicaciones y requisitos necesarios para la certificación difieren en función de estos niveles.

Para realizar la debida implementación de PCI es necesario desarrollar una documentación, como este procedimiento en la gran mayoría de implementaciones de normas estándares es un problema, es necesario desarrollar una estructura en la que se puede identificar un orden jerárquico en la generación de la documentación. Ver Figura 1.

Figura 1. Orden jerárquico en la generación de documentación.

Fuente: PCIHispano.com

9.2 PA-DSS (*Payment Application Data Security Standar*)

PA-DSS (Aplicaciones de Pago Estándar de Seguridad de Datos); es un modelo de seguridad que define requerimientos que deben cumplir las aplicaciones de pago electrónico vendidas a terceros.

Los requerimientos que certifica PA-DSS, es sobre productos que son comercializados, es decir no hechos para un solo cliente, sino que sean

aprovechados y utilizados, por su propio proveedor o cliente.

Los PA-DSS no solo se centran en las funcionalidades de *Software* sino que corroboran al proveedor de *Hardware* que tiene el esfuerzo para proteger los datos de los clientes o titulares de las tarjetas, reduciendo esfuerzos y costos, para los proveedores a la realización de una evaluación de las PCI-DSS.

A través de la combinación de PCI-DSS y PA-DSS, deben cumplir con los siguientes requisitos:

1. Empaquetar la aplicación para su distribución, confirmando que funcionara solo en la terminal de *Hardware* donde se ejecutara.
2. Soporte para apoyar algún incumplimiento de PCI-DSS del cliente.
3. Apoyo continúo a las actualizaciones de mantener el cumplimiento de las PCI-DSS.
4. El vendedor debe proporcionar información requerida para su uso con la aplicación, si se vende por separado, distribuido o con su licencia para los clientes; en conformidad con su PA-DSS en la lista de validación.

Por parte del estándar PCI-DSS para obtener la certificación en PA-SSD, se necesita realizar los siguientes pasos:

1. Realizar un análisis del manual de la aplicación identificando si el nivel de detalle técnico en los despliegues son los adecuados, los tiempos para dar respuesta si alcanzan, etc.
2. Plasmar el laboratorio de pruebas donde se desarrollaran las pruebas técnicas alineadas con los requerimientos de PA-DSS que exige en los procedimientos de auditoria y que debería de tener en cuenta el manual.
3. Documentar el resultado en el proceso de aceptación de los productos certificados.

9.3 PAN (*Primary Account Number- Número de Cuenta Principal*)

La característica principal de (PAN- *Primary Account Number)* es que es el elemento primario en las transacciones con tarjetas de pago.

El PCI-SSC (*Payment Card Industry Security Standars Council*), define controles de seguridad específicos a la protección de este dato.

Los siguientes controles son:

1. PCI-SSC (*Payment Card Industry Data Security Standars*), creo controles de seguridad puntuales para la protección del PAN y que se pueden aplicar a

cualquier entidad que lo almacene, procese, transmita o visualice.

2. PA-DSS (*Payment Application Data Security Standard*), define controles solamente los más necesarios a ser aplicados antes, durante y después de desarrollar aplicaciones licenciadas por parte de distribuidores o terceros que poseen el PAN.

Estándar PCI-DSS, el requisito 3.4 solo se aplica al PAN. Si almacena el PAN con otros elementos de los datos del titular de la tarjeta, solamente el PAN debe ser ilegible de acuerdo con el Estándar PCI-DSS, el requisito 3.4. No se puede almacenar datos confidenciales de autenticación después de la autorización, así estén cifrados.

Las compañías tienen que comunicarse con sus proveedores, distribuidores o clientes, con las marcas de servicio de pago como son Amazon Payments, PagosOnline, PSE, Payulatam, Paypal, elp En Línea Pago, MercadoPago, SafatyPay entre otros; para saber si tienen almacenamiento para datos de autenticación confidenciales, antes de la autorización, para conocer sus requisitos relacionados con la seguridad, tiempo y el uso; haciendo que como mínimo queden los datos ilegibles en cualquier lugar donde se almacenen, incluyendo los datos que son almacenados en medios digitales portátiles y en registro, de forma segura si existe una justificación de negocio empleando cualquiera de los métodos que existen:

- Valores *Hash* de una vía empleando criptografía sólida (el *Hash* debe ser del PAN completo).
- Truncamiento (los valores *Hash* no se pueden usar para reemplazar el segmento truncado del PAN).
- Token y ensambladores de Índices (los ensambladores de deben almacenar de manera segura).

El objetivo de crear estos controles es proteger los datos del PAN de fraudes causados por no tener controlada la información; evitar almacenamiento intencional o no intencional de otros datos confidenciales como tarjetas de pago CVV2 y el PIN. Si se desea visualizar un número de PAN, únicamente permite visualizar los seis primeros dígitos de la tarjeta (IIN — *Issuer Identifier Number* – Número Identificador del Emisor / BIN —Bank *Identification Number* – Número de Identificación del Banco‖), incluyendo el MII —*Major Industry Identifier* – Identificador de Industria‖ identificando el tipo de industria al que la tarjeta está asociada como VISA, MasterCard, Discover, American Express, Diners Club, para efectos de enrutamiento de transacciones interbancarias; por el cual es gestionado con las normas ANSI – *American National Standards Institut*e, acelerando la aceptación de los productos con la mejor seguridad para los consumidores, y los cuatro últimos dígitos; plasmado en el requisito 3.3 del estándar PCI-DSS, de modo que solo el personal con una necesidad comercial legitima pueda ver el PAN completo. Ver Figura 2.

Figura 2. Clasificación dígitos de la tarjeta de crédito

Fuente: PCIHispano.com

IAI (*Individual Account Identification* – Identificación de Cuenta Individual), está compuesto a partir del séptimo digito hasta el penúltimo digito donde identifica el número de cuenta asociado al titular de la tarjeta.

CHECK DIGIT (Dígitos de Chequeo), es el último digito de la tarjeta. La longitud del PAN depende del servicio de marca de tarjetas que lo gestiona y el tipo de industria, Visa y visa (13 o 16 Dígitos), Mastercard (16 Dígitos), Discover (16 Dígitos), American Expres (15 Dígitos), Diners Club (14 Dígitos), Maestro (12 a 19 Dígitos – Para Tarjetas Débito Internacionales) y JCB (15 o 16 Dígitos – Para Japón).

Evaluar el almacenamiento de datos que sean ilegibles, es decir que no estén almacenados en un formato de texto claro; empleando herramientas que le permitan realizar una búsqueda de datos de tarjetas PAN como las siguientes: OpenDLP, FTimes, SENF entre otras.

9.4 TIPOS DE TARJETAS DE PAGO (CID, CAV2, CVC2, CVV2)

Los diferentes tipos de tarjetas de pago (CID, CAV2, CVC2, CVV2), traen un código de validación y es para proteger las transacciones que se realizan de forma no presencial, ya sean ejecutadas por medio de Internet, Correo Electrónico o por Teléfono, en las que ninguno de los dos actores está presentes, consumidor y tarjeta.

Si en dado caso llegase a haber un fraude de los datos por personas fraudulentas, ellos pueden hacer transacciones por los medios de Internet, Correo Electrónico o por Teléfono.

Debido a que está expuesto el riesgo de fraude, los bancos optaron por agregar el código de validación de seguridad para evitar la manipulación no autorizada que permita validar la integridad y la posesión de la tarjeta cuando se realice una

transacción no presencial. Los códigos son nombrados CVV (*Card Verification Value* – Valor de Verificación de la Tarjeta) o CVC (*Card Validation Code* – Código de Validación de Tarjetas), es almacenado en la Pista 2 de la banda magnética y no es visualizada por el dueño de la tarjeta, debido a que la validación del código es automática cuando el banco recibe una transacción.

La información que almacena el código de validación es la fecha de expiración de la tarjeta y el código de servicio encriptados usando dos llaves; el código se genera en el momento de la estampación de la tarjeta utilizando el PAN.

Algunas tarjetas de pago aún se realizan transacciones empleando banda magnética, estos datos son enviados y procesados por el banco y comparados con una base de datos de referencia para verificar su integridad, si los datos coinciden eficazmente quiere decir que no han sido manipulados y se trató de una transacción legítima y exitosa.

Las marcas de tarjetas les dieron un nombre diferente a los códigos:

1. CAV (*Card Authentication Value* – Tarjetas JCB).
2. CVC (*Card Validation Code* – Tarjetas MasterCard).
3. CVV (*Card Verification Valu*e – Tarjetas de Visa y Discover).
4. CSC (*Card Security Code* – Tarjetas American Express).

Los bancos y los comercios, continúan con una operatividad ante un problema al que no le encuentran una solución a largo plazo para las compras realizadas por teléfono. Toda esta dificultad es porque el número que está impreso es visible y dictado por el cliente a una persona de servicio quien la envía al banco para su validación. Cualquier persona que conociera un PAN podría realizar una compra suplantando al dueño de la tarjeta.

La solución más práctica al problema fue emplear el mismo concepto de CVV y estamparlo en la tarjeta para que el cliente pudiera visualizarlo, y así dictaba por teléfono el número de su tarjeta PAN, la fecha de expiración y el código CVV impreso a la persona del servicio. Los datos eran enviados al banco y mediante una comparación podía verificar si la tarjeta era integra o no sin necesidad de realizar una lectura directa de la banda magnética.

Se opta por darle un nombre diferente a este nuevo código almacenado en la banda magnética para diferenciarlo dependiendo de la marca de tarjetas:

1. CID (*Card Identification Number* – Tarjetas American Express y Discover).
2. CAV2 (*Card Authentication Value* 2 – Tarjetas JCB).
3. CVC2 (*Card Validation Code* 2 – Tarjetas MasterCard).
4. CVV2 (*Card Verification Value* 2 – Tarjetas Visa).

En conclusión los códigos (CAV, CVC, CVV, CSC) se encuentran asociados a la información de seguridad almacenados en la banda magnética y los códigos (CID,

CAV2, CVC2, CVV2) los valores de seguridad se encuentran estampados en la tarjeta para realizar transacciones no presenciales.

De acuerdo al uso de Internet, comercio electrónico y las compras On-Line, los códigos (CID, CAV2, CVC2, CVV2), se toma la decisión para realizar transacciones sin tarjetas físicas, es por tal razón que cuando realicen una compra por medios On-Line el comercio solicitara el código para verificar la posesión e integridad de la tarjeta.

9.5 LONGITUD Y UBICACIÓN DE LOS VALORES (CID, CAV2, CVC2, CVV2)

El valor CVV2 es un numero de tres dígitos en las tarjetas VISA, MasterCard y Discover, tarjeta crédito y débito. La tarjeta American Express tiene un código de cuatro dígitos, tarjetas crédito o débito. Ver la Figura 3.

Figura 3. Longitud y ubicación de los valores del CVV.

Fuente: cvvnumber.com

9.6 PRUEBAS O CONSIDERACIONES DE SEGURIDAD CON (CID, CAV2, CVC2, CVV2)

Revisar las fuentes de datos corroborando que el código o el valor de verificación de la tarjeta de tres o cuatro dígitos impreso en la tarjeta los datos (CID, CAV2, CVC2, CVV2) no se almacene después de la autorización validando: Datos de transacciones entrantes, todos los registros, archivos de historial, archivos de

seguimiento, esquemas de base de datos y contenidos de base de datos.

9.7 ESTÁNDAR PCI-SSC Y LAS TARJETAS DE PAGO (CID, CAV2, CVC2, CVV2)

Debido a la confidencialidad el estándar PCI-SSC en el requisito 3.2.2, no almacenar el valor ni el código de validación de las tarjetas que se usa para verificar las transacciones de las tarjetas no presenciales, implica que el proveedor o el comercio de servicio solicite al usuario el (CID, CAV2, CVC2, CVV2) en cada transacción que realice. Es muy importante para que sea implementado en las compañías y así evitar fraudes al momento de realizar una transacción no presencial, permitiendo autenticación y validación de integridad con los dueños de las tarjetas.

9.8 PIN (*Personal Identification Number* – Número de Identificación Personal)

Es una protección llamada PIN, que se realiza mediante la transmisión entre el dispositivo de encriptación del PIN y la CPI lector.

Si los dispositivos de encriptación no están integrados en el mismo modulo y el método de verificación es titular de la tarjeta se determina que son un PIN cifrado, el bloque del PIN y el lector ICC ha utilizado un autenticado clave de cifrado de la tarjeta de CI, o de acuerdo a la norma ISO9564, donde el objetivo de la gestión PIN es protegerse contra la divulgación no autorizada.

Es necesario garantizar que durante su ciclo de vida, que consiste en la activación, selección, emisión, activación, almacenamiento, y cualquier otro uso que se realice, estén en todo momento.

Mantener el secreto de las claves de cifrado es de mayor importancia. Siempre que sea posible, tener en cuenta la norma ISO9564, por la cual especifica los requisitos.

9.9 DMZ (*Demilitarized Zone*)

El DMZ o red perimetral, es básicamente una zona de seguridad, donde se puede iniciar dentro de la red interna de un usuario (Empresa u organización), que se extiende hacia una red externa, la cual generalmente es en internet.

El principal objetivo del DMZ, es dar acceso y verificar que las conexiones entre la

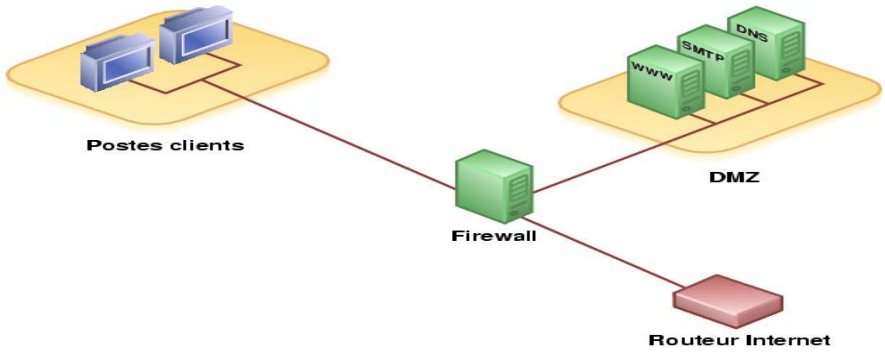
red interna y le red externa, estén autorizadas y permitir dicha conexión, además, las conexiones desde la DMZ solo están permitidas a la red externa, no se encuentran permitidas las conexiones de equipos (hosts) a la red interna.

La forma de controlar las conexiones que se realizan desde la red externa hacia la DMZ, es utilizando *Port Address Translation* (PAT) – Traductor de conexiones TCP y UDP realizadas desde una red externa, mediante un host y un puerto a otra dirección de una red interna.

La DMZ, guarda cierta vulnerabilidad, hacia riesgos muy críticos, teniendo en cuenta, que son servidores de servicio al cliente externo, como *FrontPage*, FTP (*File transfer protocol)*, entre muchos otros, que se encuentran expuestos al internet y redes externas, por ello, es necesario proteger e implementar soluciones que garanticen la protección de la DMZ.

En cuanto una DMZ, sea implementada, esta debe tener un diseño de seguridad que permita garantizar que no será vulnerada y que puede ser transitada sin riesgos. A continuaciónse puede observar una red típica que usa un DMZ con un *firewall*. Ver Figura 4.

Figura 4. Red MZ (DMZ *Demilitarized Zone*)



Fuente: es.scribd.com

9.10 *FIREWALLS*

El *Firewalls* o corta fuegos en español, básicamente hace parte de un sistema o una red, controla puertos y conexiones, con el cual se restringe el acceso no autorizado, que a su vez, permite las comunicaciones que se encuentren autorizadas, está muy relacionado en el DMZ, como se puede apreciar en la Figura 4; es una herramienta

o parte del sistema, que permite establecer una comunicación, entre las redes internas y externas, con un mayor grado de seguridad.

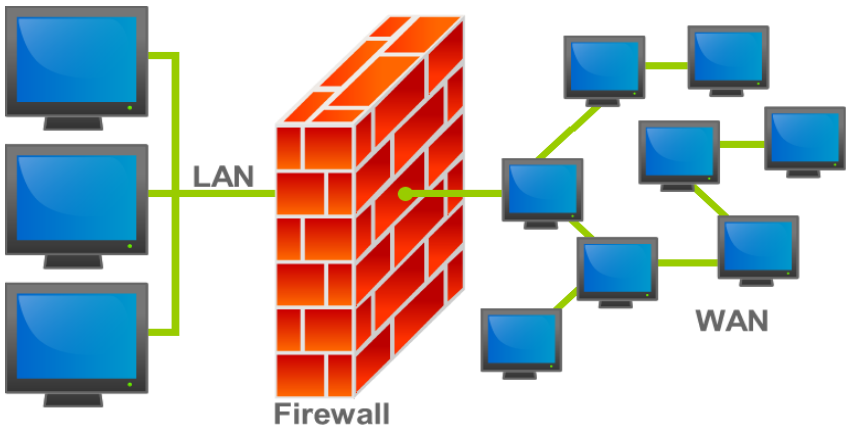
Enruta, reenvía, direcciona y realiza filtros de datos que tienen tránsito de una red a otra, no permite que los usuarios accedan a host no autorizados, que pueden traer riesgos informáticos a la organización.

Estos pueden ser, conformados por un dispositivo o varios dispositivos, que deben permitir la implementación de seguridad, donde se permita cifrar, permitir, descifrar etc. bajo las normas, protocolos u otros criterios, que el usuario requiera para disminuir el riesgo en la seguridad informática.

Se encuentran varios tipos de corta fuegos. Ver Figura 5:

- **Entrante:** Este se encarga de controlar todas aquellas conexiones entrantes a la red, verifica direcciones IP que se quieran conectar a la red.
- **Saliente:** Verifica todas las conexiones salientes, que se conectan a un servidor, controla las direcciones IP a las cuales se quieran conectar desde la red.
- **Controlar el tipo de conexión:** Se encarga de identificar conexiones extrañas, que pretendan confundir al sistema, para intentar violar la seguridad del mismo, con esto pueden intentar establecer conexiones confusas, incompletas u otro tipo de conexión, que permita transgredir la seguridad de la red.
- **Controlar la denegación de servicio:** Básicamente, este control se activa, cuando quieren saturar la red con conexiones que superan el número limitado, lo que hace el este control, es identificar la saturación y denegar los accesos que estén produciendo esta situación.

Figura 5. *Firewalls*



Fuente: Etapa.net.ec

9.11 Estándares

9.11.1 CIS. Acrónimo de "*Center for Internet Security*" (Centro de Seguridad en Internet). Empresa sin fines de lucro cuya misión es ayudar a las organizaciones a reducir el riesgo de interrupciones en su negocio y en el comercio electrónico provocado por controles de seguridad técnicos inadecuados.

9.11.2 ISO "*International Organization for Standardization*" 27001. Esta norma, tiene alcance para todo tipo de organizaciones, fue creada, para proporcionar un modelo para establecer, implementar, operar, revisar, monitorear y mejorar el ISMS (*Information Security Management System*), o en español, el Sistema de Gestión de Seguridad de la Información.

La implementación de la ISMS, es básicamente una decisión estratégica de la organización, el cual está basado, en las necesidades, tamaño de la organización y estructura de la misma, acarreando la necesidad de requerimientos de seguridad, procesos, dinámicas de implementación y soluciones.

Esta norma ISO, adopta el modelo "*Plan – Do – Check – Act*" o PDCA, el cual se aplica a todas las estructuras de los procesos ISMS, por medio del "PLAN" – se debe establecer el ISMS, en la cual debe contener políticas, objetivos, procesos, procedimientos que sean relevantes, para la distribución del riesgo y cualquier mejora a la seguridad de la información, obteniendo resultados acorde a las políticas y objetivos establecidos.

"*DO*" – aquí se refleja la adecuada forma de implementar y operar el ISMS, por medio de políticas, controles, procesos y procedimientos.

"*CHECK*" – básicamente, aquí se efectúa la revisión de los procesos, en donde se evalúan el cumplimiento de los objetivos y políticas, generando un informe de los resultados a la administración.

"*ACT*" – aquí se procura mantener y tener planes de mejoramiento del ISMS, por medio de acciones correctivas, derivados de auditorías internas y las respectivas revisiones al ISMS.

Esta norma tiene las siguientes cláusulas que conforman su articulación:

1. ISMS
2. Responsabilidad de la administración
3. Auditoría interna del ISMS
4. Administración de las revisiones ISMS
5. Mejoramiento continuo al ISMS

Si hay algún tipo de exclusión de algún control detallado, esta exclusión debe estar justificada y debe evidenciar las razones por las cuales estos riesgos son asumidos y aceptados, al excluir cualquier tipo de control.

Todos los documentos, que sean requeridos por el ISMS, deben estar protegidos y deben encontrarse controlados, todas sus revisiones, cambios, y actualizaciones deben quedar totalmente documentadas.

La responsabilidad de la administración, es proporcionar las herramientas necesarias, para el establecimiento, mantenimiento y mejora del ISMS, a través de políticas, objetivos, planes, establecimiento de responsabilidades, comunicación y sensibilización de la organización, de la importancia y apoyo necesario, para el cumplimiento de dichos objetivos.

Se deben contar, con personal idóneo, competente y capacitado, para realizar las actividades requeridas, para lograr los objetivos propuestos.

La organización, por medio de la administración, debe organizar, auditorías internas al ISMS, por medio de una planeación, en donde se verifique que los controles, políticas y objetivos se cumplen según lo especificado, esto debe realizarse al menos una vez al año, para mantener la vigencia, adecuación y efectividad al ISMS. Se deben presentar mejoras continuas, que permitan obtener una mayor eficiencia, por medio de los resultados de las auditorías, en caso de presentarse desviaciones en las políticas, objetivos y procesos, se deben implementar planes de acciones o correctivos, que permitan evitar que se puedan repetir.

9.11.3 ISO "*International Organization for Standardization*" 27005. Esta Norma está alineada a la ISO 27001 encargándose de la gestión de riesgos SGSI (Sistema de Gestión de Seguridad de la Información), en todo tipo de empresa en seguridad de la información en su organización, identificando las necesidades, las amenazas que están expuestos los activos y el impacto que genere en la compañía.

En el alineamiento del Sistema de Gestión de Seguridad de la Información y el Proceso de Gestión del Riesgo en la Seguridad de la Información está la metodología PHVA (Planear: Planificar el tratamiento del riesgo, Hacer: Implementar el tratamiento del riesgo, Verificar: Realizar monitoreo continuo y revisión de los riesgos, y Actuar: mantener y mejorar el proceso de riesgo). Consiste en definir estrategias en las organizaciones estableciendo criterios de evaluación, estructura de análisis, roles y responsabilidades, criterios de impacto y de aceptación del riesgo.

Es muy importante identificar el alcance y límites, para así saber hasta dónde se puede atacar y objetivo del riesgo.

En cuanto a las responsabilidades de gestión del riesgo y la seguridad de la información se recomienda definir las funciones, establecer relaciones entre las partes y la organización, definir rutas para escalar decisiones de la organización.

Para reducir el riesgo se deben considerar varias restricciones al seleccionar controles adecuados teniendo en cuenta los criterios de aceptación del riesgo, como: Restricciones de tiempo, financieras, técnicas, controles nuevos, operativas, éticas, etc.

Se pueden tomar decisiones para evitar el riesgo mediante el retiro de una o varias actividades, o el cambio como operan las actividades. En cuanto a los riesgos residuales en algunos casos es posible que no sean exitosos en la aceptación del riesgo porque no son prevalentes en algunas circunstancias.

El proceso de evaluación detallada es la identificación profunda de las amenazas y vulnerabilidades de los activos, el resultado de esta evaluación se usa para evaluar los riesgos e identificar su tratamiento de riesgo.

9.11.4 SANS. Acrónimo de "*SysAdmin, Audit, Networking and Security*" (Administración de sistemas, auditorias, redes y seguridad), un instituto especialista en capacitación en seguridad informática y certificación profesional. (Consulte www.sans.org.)

9.11.5 NIST "*National Institute of Standards and Technology*" (Instituto Nacional de Normas y Tecnología). Vale aclarar que NIST, tienen como misión principal, la promoción de la innovación y la competencia industrial, todo esto mediante la implementación de medidas para la ciencia, normas y nuevas tecnologías, en procura de mejorar la calidad de vida.

Básicamente la NIST 800-53, aborda la selección de controles de seguridad para los sistemas de información federales (EEUU), bajo los requisitos de seguridad FIPS 200, como parte clave para la certificación y acreditación de los sistemas de información federales, es elegir subconjuntos de controles o salvaguardas, tomados del catálogo de control de seguridad (NIST 800-53, en su apéndice F).

La función de estos controles es, proteger la confidencialidad, integridad, y disponibilidad del sistema y la información que contiene.

Sin embargo, revisando la última versión 4, en donde se observa, que se actualiza debido a la asociación de seguridad de la información cibernética, entre el departamento de defensa de EEUU, la comunidad de inteligencia, y las agencias civiles federales, NIST realizó una publicación especial sobre el control de seguridad y privacidad para sistemas y organizaciones federales, en donde se actualizaron y mejoraron los controles y sistemas de seguridad, se enfocaron estrictamente en las

amenazas internas de la información, seguridad en las aplicaciones del *software* incluyendo las páginas web, redes sociales, todos los dispositivos móviles y las llamadas "*Cloud*", las soluciones de dominio cruzado, amenazas avanzadas, seguridad en la cadena de suministro, los sistemas de control industriales y de procesos y por último la intimidad.

Viéndolo así, en conclusión, NIST 800 – 53 V4, trata de disminuir a su mínima expresión, el riesgo informático para las entidades de defensa, inteligencia y organizaciones federales de los EEUU, por medio de estrictos controles de seguridad cibernética de la información.

9.11.6 NIST *Special Publication* 800-115 -*Technical Guide to Information Security Testing and Assessment* (Guía Técnica para la Información de Pruebas de Seguridad y Evaluación). Esta guía determina como una organización cumple con los objetivos de seguridad cuando se evalúa. Existen tres métodos para evaluar: pruebas, examen y entrevista.

- Pruebas: Es el proceso encargado de evaluar específicamente su comportamiento real en la organización.
- Examen: Es comprobar, revisar, inspeccionar o analizar objetos de la evaluación y así lograr comprender más y obtener evidencias.
- Entrevista: Se lleva a cabo discusiones dentro de la organización y así lograr mejor comprensión, aclaraciones para llegar a la evidencia.

La suma de estos tres métodos da un resultado de la evaluación para apoyar la eficacia del control de seguridad con la restricción del tiempo.

Esta técnica de pruebas, examen y técnicas, las organizaciones las pueden usar en las evaluaciones y sus asesores en la parte de ejecución, obteniendo un impacto en los sistemas y redes, deben admitir el proceso técnico para que la evaluación sea exitosa.

La guía permite que las organizaciones implementen políticas de evaluación de seguridad, restricciones, roles, metodologías, que permitan tener una relación técnica de evaluación.

Muestra un plan de asesoría y de evaluación, de información técnica para determinar orientación en el proceso de evaluación.

Tiene una forma segura y eficiente de evaluación, con capacidad de resolver cualquier incidente que pueda ser presentado en la evaluación.

Dirige muy bien la parte técnica en cuanto al almacenamiento, recolección, transmisión y destrucción, en el proceso de evaluación.

Saca informes de sus respectivos análisis evidenciando resultados técnicos para mitigar riesgos y así mejorar la seguridad en las organizaciones.

La NIST recomienda a las organizaciones realizar las evaluaciones técnicas para proporcionar el mayor valor estableciendo una política de evaluación de seguridad de información, implementar una metodología documentada, determinar los objetivos de cada evaluación, analizar los resultados y desarrollar técnicas para mitigar los riesgos.

9.12 *HASH FUNCTION USAGE*

Esta función se utiliza cuando en algunas aplicaciones, se requieren abreviar algunos mensajes, se le llama mensaje truncado y solo se puede usar la función *hash*, si la longitud del bloque de salida, es mayor que λ (es decir, L> λ), también los λ que se encuentren más a la izquierda, serán seleccionados como el resumen del mensaje truncado y los bits más hacia la derecha se descartan, eso depende, de la extensión en bits, que el usuario quiera tener en el menaje truncado, sin embargo, según las normas y recomendaciones NIST, truncar los mensajes, pueden traer como consecuencia la afectación de la seguridad.

Esta función *hash*, también se maneja, para la utilización de firmas digitales, así como se desarrolla una operación de clave privada, que produce una firma digital, esta es utilizada, como verificación de la identidad de quien firma el mensaje y si este mensaje presenta algún tipo de alteración, luego de su firma.

Cuando dos mensajes presentan el mismo resumen, se presenta la llamada “Colisión”, aquí se puede estar utilizando una firma para intentar autenticar un mensaje, el cual no es el original, lo cual implica que una firma autenticada, no garantiza la autenticidad el mensaje que se encuentra firmado, así entonces, una función *hash*, debe tener resistencia a la colisión, para evitar este tipo de riesgos.

Se encuentran tres funciones *hash*, las cuales son:

- **Datos de entrada con MD5**: aquí el algoritmo realiza un resumen de 128 bites a los mensajes que no tienen longitud sin definir. Este es utilizado, en la creación de resúmenes codificados en base 64.
- **Datos de entrada con SHA-1**: genera un mensaje resumen de 160 bits, tomando un mensaje de entrada inferior a 264 bits. Este es utilizado, en la creación de resúmenes codificados en base 64.
- **Dispersión de los datos con SHA-256**: toma un documento para el que desea generar el resumen y le da la longitud que requiera. Este es utilizado, en la creación de resúmenes codificados en base 64.

9.13 TRUNCAMIENTO

El truncamiento, es un método el cual se utiliza para eliminar segmentos del PAN ("*primary account number*" – "número de cuenta principal"), este es un número exclusivo de una tarjeta de pago (Débito o Crédito), con este truncamiento el PAN, se convierte en un número completamente ilegible.

Este truncamiento, se utiliza cuando se almacena la información en archivos, data base, recibos impresos, pantallas, etc.

9.14 TOKEN CRIPTOGRÁFICO O TOKEN DE SEGURIDAD

El token criptográfico o de seguridad, es un dispositivo, el cual se utiliza para realizar la validación de los usuarios autorizados a un servicio, que permite realizar un proceso de autenticación, no solo de usuario, también de permisos especiales, para realizar transacciones en la red.

Son de tamaño pequeño, de fácil transportación, pueden utilizarse o llevarse como llaveros, en ellos pueden almacenarse claves criptográficas como son: firmas digitales o huellas digitales (Datos biométricos), entre los token más conocidos se encuentran los que generan claves dinámicas "OTP – *One time password*" (Por ejemplo, los entregados por los bancos a los usuarios, como empresas), también están los token USB, en donde comúnmente se pueden almacenar contraseñas, certificados y poder acceder a la identidad de la persona. Ver Figura 6.

Figura 6. Token Criptográfico.

Fuente: salmoncorp.com

9.15 CRIPTOGRAFÍA SÓLIDA

Esta criptografía se basa en algoritmos, que han sido probados exitosamente y reconocidos por la industria.

Aquí se extienden las claves sólidas y se realizan las buenas y adecuadas prácticas de administración de claves. Este es un método de protección de datos, en donde se tienen en cuenta los cifrados reversibles (Ejemplo: hashing), los no reversibles o de un único uso.

Algunas normas aprobadas son:

- AES (128 bits y superior)
- TDES (claves mínimas de doble extensión)
- RSA (1024 bits y superior)
- ECC (160 bits y superior)
- El Gamal (1024 bits y superior).

9.16 CMMI (*Capability Maturity Model Integration*) O INTEGRACIÓN DE MODELOS DE MADUREZ DE CAPACIDADES

Son modelos desarrollados, bajo lineamientos específicos, para evaluar los desarrollos, mantenimiento, procesos y la correcta operación del *software*. Su última versión es la 1.3, las áreas en las cuales se enfocan estos modelos son el desarrollo, la adquisición y los servicios.

Así se tiene que los modelos son los siguientes:

- Desarrollo: (CMMI-DEV o CMMI *for Development*), V - 1.2.
- Adquisición: (CMMI-ACQ o CMMI *for Acquisition*), Versión 1.2.
- Servicios: (CMMI-SVC o CMMI *for Services*).

Se debe tener en cuenta, que estos modelos, deben ser adaptados según el negocio o los objetivos de negocio de cada organización.

Estos modelos, no sirven para que las organizaciones sean certificadas, por lo general, las organizaciones son evaluadas, por ejemplo, por medio de una evaluación SCAMPI (*Standard CMMI Appraisal Method for Process Improvement*), de donde recibe una calificación de 1 a 5, consecuente a los niveles de maduración que presente.

Estos son los niveles de calificación que se pueden obtener, mediante esta evaluación:

N1: No confiable – se maneja un ambiente impredecible, donde no hay controles o actividades de control diseñadas por parte de la organización.

N2: Informal – Se verifica que existen actividades de control, sin embrago, no se llevan a la práctica, estas actividades, las realizan las personas sin ningún entrenamiento formal y no existe comunicación sobre las actividades.

N3: Estandarizado – existen actividades de control, se encuentran diseñadas y documentadas, además se han comunicado a los empleados, puede que hallan desviaciones que no se puedan detectar.

N4: Monitoreado – Para soportar las actividades de control, se utilizan herramientas o ayudas limitadamente.

N5: Optimizado – Existe una estructura que integra de forma adecuada el control interno, que es monitoreado por la gerencia, de aquí se derivan las mejoras continuas, y se realizan planes de acción al momento de detectar errores en el manejo de las personas o en las actividades realizadas.

Vale anotar que las organizaciones miden su progreso mediante la evaluación (appraisal), en la cual pueden ganar niveles de madurez, o de capacidad de logro.

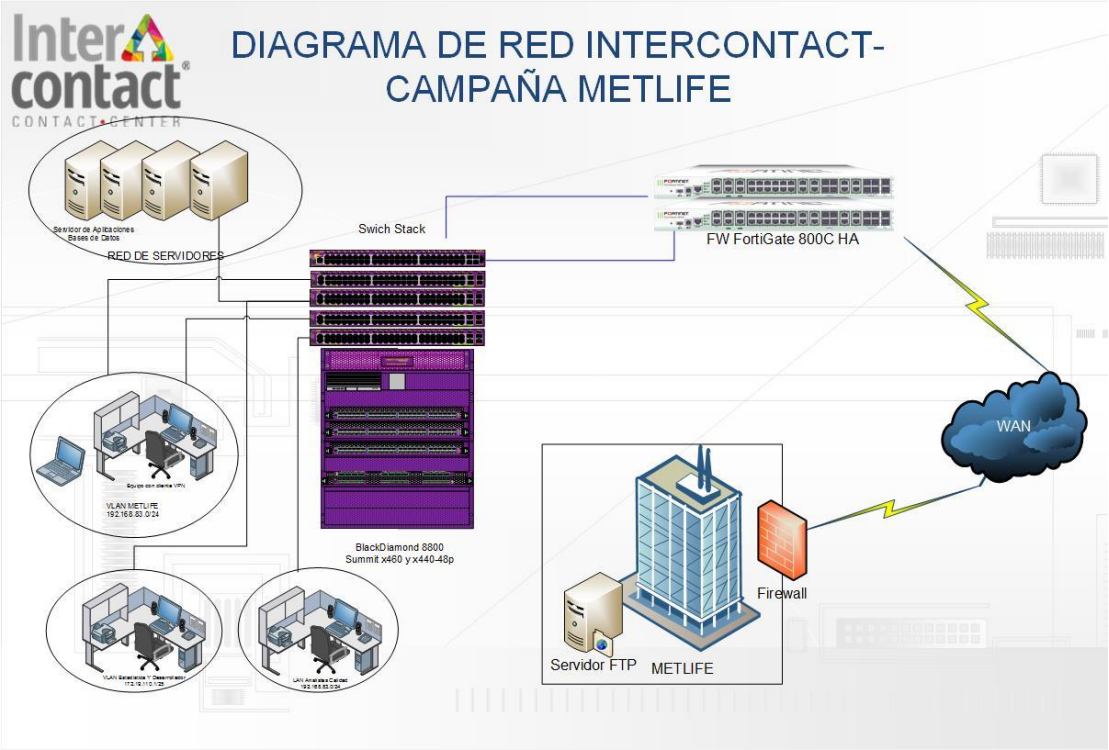
Esta evaluación se realiza, por razones como el llegar a determinar qué tan saludables se encuentra los procesos de la organización, respecto a las mejores prácticas CMMI, identificando las mejoras que pueden realizarse, también, para cubrir los requisitos de clientes públicos o privados, mediante licitaciones.

Hay tres clases de evaluación: A, B y C, la única evaluación formal es la “A”, ya que es la única evaluación con nivel.

10. ESTADO ACTUAL INTERCONTACT

10.1 DIAGRAMA DE RED ACTUAL

Figura 7. Diagrama de Red Actual Intercontact



Fuente: Elaboración propia, 2017

El diagrama de red de Intercontact que involucra el almacenamiento, transmisión y procesamiento de datos del titular de la tarjeta, se puede evidenciar aspectos fundamentales que generan incumplimiento con la PCI-DSS como son la trasmisión en plano de los datos, varias áreas de la empresa manipulan los datos del titular, toda la red de servidores está alojada en una sola vlan, entre otros aspectos que se explicaran con mayor detalla en el diagnóstico generado con el análisis GAP. Ver Figura 7.

10.2 CRITERIOS DE EVALUACIÓN

Para realizar un adecuado análisis GAP en la compañía con el fin de determinar

cuál es el estado actual y el estado deseado relacionado con el cumplimiento de la norma PCI en Intercontact en la campaña Metlife se toma como base una metodología CMMI (Modelo y capacidad de madurez) que consiste en calificar cada área definida de seguridad sobre una escala de 0 a 5 con base a la madurez de los procesos. Este proceso permite a la organización aclarar su visión, estrategia y como llevarlas a cabo, además de ofrecer retroalimentación sobre los procesos internos del negocio y los resultados externos para continuar mejorando el desempeño estratégico de la compañía.

Estos niveles están representados en los siguientes estados. Ver Cuadro 2:

Cuadro 2. Modelo de la capacidad de madurez

Estado	Valoración	Significado
No existe	0	No cuenta con el procedimiento o control definido por la norma.
Inicial	1	Se reconoce la necesidad pero no se han identificado los mecanismos para implementar los controles
Repetible	2	Se ejecutan los controles pero no están documentados, se depende de la disponibilidad del responsable del control para su ejecución
Definido	3	El control está documentado, se ha divulgado, pero no se realizan mediciones de su desempeño
Gestionado	4	Se han definido los límites dentro de los cuales debe operar el control, se evalúa el desempeño y se generan informes
Optimizado	5	Se incorporan las mejores prácticas de la industria y las métricas de los controles se consolidan en herramientas estratégicas de toma de decisiones, ejemplo *Balance Score Card*
No Aplicable		Los controles no son aplicables a la actividad o proceso
Fuente: Basado de CISM (Capítulo de Gobierno de seguridad de la información)		

10.3 ANÁLISIS GAP

Un análisis GAP ayuda a identificar la distancia entre el estado real de INTERCONTACT frente a la PCI-DSS y el cumplimiento de la norma PCI-DSS. Este análisis ayudara a identificar las necesidades de la organización, tener una visual sobre la planificación en tiempo e inversión para conseguir estos objetivos de cumplimiento.

A continuación, se muestra el análisis GAP desarrollado para Intercontact que muestra las actividades, tareas, procedimientos, políticas, infraestructura y cambios que debe realizar respecto a la situación actual que tiene la compañía con el fin de dar cumplimiento a PCI-DSS. Ver Cuadro 3:

Cuadro 3. Análisis GAP – Intercontact

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
Requisito 1:	**Instale y mantenga una configuración de *firewall* para proteger los datos del titular de la tarjeta.**			
1.1	**Establezca e implemente normas de configuración para *firewalls* y *routers* que incluyan lo siguiente**	Inicial	La compañía actualmente cuenta con dos *firewalls* en cada sede configurados en alta disponibilidad	Se debe crear normas o procedimientos de configuración del *firewalls* para la implementación de campañas o perfiles.
1.1.1	Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los *firewalls* y los *routers*	Repetible	Existe un procedimiento de solicitud y ejecución cuando se requiere permisos a Internet mediante una herramienta de mesa de ayuda, no existe un procedimiento formal de aprobación de estos permisos, muchos de las solicitudes en nuevas implementaciones requieren manipulación de políticas y parámetros del *firewall* como son la vpn, estas no cuentan con plan de trabajo donde se apruebe el respectivo cambio. No existe un procedimiento documentado donde se pruebe ciertas manipulaciones del *firewall*	Implementar un procedimiento de aprobación y pruebas para cambios configurados en el *firewalls* relacionado a VPNs, implementación de application control, entre otros.
1.1.2	Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.	Inicial	Existen diagramas de red en los que se muestra las conexiones WAN, enlaces, dispositivos de red de la compañía y servidores	Realizar diagrama de red donde se muestre detalles de la estructura tecnológica a nivel de red LAN (vlans, acls, redes inalámbricas, conexión a servidores, *stac*ks, todos los dispositivos de red y demás), donde se documente todas las conexiones que existen entre los datos de los titulares de la tarjeta.
1.1.3	El diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes.	No existe	No existe un diagrama de flujo donde se evidencie los datos de titulares de tarjeta entre los sistemas y las redes, no se identifica claramente donde se ubican estos datos, se procesan y por donde se transmiten estos datos.	Realizar diagramas de flujo de datos donde se evidencie el flujo de datos de los titulares de las tarjetas donde se identifiquen parámetros como almacenamiento, transporte, redes, dispositivos, estaciones de trabajo involucradas en el transporte, almacenamiento de los mismos.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
1.1.4	Requisitos para tener un *firewall* en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.	Repetible	La compañía cuenta con dos *firewall* configurados en alta disponibilidad, estos dispositivos segmentan la red LAN de la WAN (enlaces hacia otras sedes o compañías, internet, vpns), también segmentan la red LAN de la DMZ. Existe diagramas de red en la compañía, pero falta el detalle de cómo está de acuerdo a los parámetros de configuración que tiene el *firewall*. No existen normas de configuración documentadas del *Firewall*.	Actualizar los diagramas de red de la compañía con detalle de los parámetros de configuración que tiene el *firewall*. Se debe documentar las normas de configuración del *firewall*.
1.1.5	Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.	Repetible	Está definido el rol de administrador del *firewall* y quien es el encargado de administrarlo, pero no está documentado la descripción de roles y responsabilidades de quienes acceden al *firewall* y las responsabilidades puntuales para la administración de los dispositivos de red.	Realizar la documentación sobre la descripción de roles y responsabilidades de quienes acceden al *firewall* y las responsabilidades puntuales para el administrador de los dispositivos de red.
1.1.6	Documentación y justificación de negocio para el uso de todos los servicios, protocolos y puertos permitidos, incluida la documentación de las funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros.	Inicial	Se identifican y generan controles en la implementación de políticas, rutas, puertos, permisos y demás en el *firewall*, pero no existe documentación formal de la configuración. No se identifica las funciones de seguridad de cada servicio configurado. La campaña Metlife tiene definido los puertos, servicios, rutas y permisos específicos pero no están debidamente documentados. Algunos perfiles como el de los supervisores tiene ciertos permisos con ciertos privilegios que no están debidamente definidos ni documentados, ni justificados	Se debe definir y documentar todos los servicios, protocolos, puertos, rutas y demás de manera formal y justificada de cada campaña en especial la campaña de Metlife con las respectivas funciones de seguridad de cada servicio configurado. Asegurar que deshabiliten o eliminen el resto de los protocolos, servicios y puertos que no son necesarios para la ejecución normal de la campaña. Todos estos servicios deben ser aprobados por un funcionario ajeno al que realizo la debida configuración en el *firewall*. En caso que se necesite utilizar ciertos servicios, puertos o funciones inseguras, este riesgo tiene que estar definido y debidamente tratado para que de esta manera se pueda utilizar estos privilegios de manera segura.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
1.1.7	Requisito de la revisión de las normas de *firewalls* y *routers*, al menos, cada seis meses.	Inicial	Existen revisiones mensuales en la configuración del *firewall* en aspectos como políticas, rutas, *webfilters*, *application control, ips,* entre otros, pero esta revisión no es comparada con la documentación o solicitud formal identificando si estos servicios realmente están configurados y aprobados de manera correcta. Aunque la revisión esta de manera documentada no existe el detalle de los aspectos que fueron revisados en las políticas de la campaña Metlife u otra.	Se debe realizar de manera formal y medible la revisión de las normas de configuración del *firewall* (políticas, rutas, *webfilters, application control*, puertos, etc.) mínimo cada seis meses de las debidas campañas (Metlife) en comparación a la implementación o solicitud formal de la misma. Se debe evidenciar de igual manera la depuración o eliminación de elementos que ya no son necesario, o actualizar los mismos, en busca que solo se esté otorgando permisos o privilegios debidamente autorizados y justificados con el negocio.
1.2	**Desarrolle configuraciones para *firewalls* y *routers* que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas.**	Repetible	Las conexiones hacia redes no confiables o externas están debidamente bloqueadas o configurada. La red LAN está debidamente segmentada de las redes externas (WAN, DMZ, enlaces) mediante un *firewall* en alta disponibilidad, configurada con diferentes vdoms Hay configurados parámetros en la políticas con *traffic shapers* en algunas políticas.	Verificar que todas las conexiones a la fecha hacia redes no confiables o externas estén debidamente configuradas.
1.2.1	Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.	Inicial	El *firewall* está configurado de manera que todo el tráfico tanto entrante como saliente esta por defecto en ***deny*** El *firewall* cuenta con normas de configuración que identifican el trafico entrante y saliente de la campaña Metlife y las otras campañas, en aspectos como puertos, servicios, políticas, rutas, interfaces. Los analistas de estadística y calidad tiene cierta manipulación y acceso a la información de los datos de los titulares y de las tarjetas no tienen bien definido el tipo de privilegios a los que tienen de acceso: servicios, protocolos, páginas, entre otros.	Configurar la campaña Metlife para que se restringa la cantidad necesaria de tráfico tanto entrante como saliente y documentar el mismo. De debe restringir para que el perfil de los analistas de calidad y de estadística manipulen la información del titular y números de la tarjeta. Si esta va a ser manipulada en algún punto esta información debe estar cifrada. Se deben definir claramente el perfil de los analistas relacionado a los servicios, puertos, IPs a las que tenga conexión y rutas.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
1.2.2	Asegure y sincronice los archivos de configuración de *routers*.	Repetible	La compañía tiene un Core capa 3, donde los cambios son guardados pero no documentados. Estos cambios guardados garantizan que el archivo de configuración en ejecución sea el mismo cuando el dispositivo se reinicie. Este archivo de configuración tiene un backup que se ejecuta semanalmente. En el *firewall* de la compañía se configura todas las rutas estáticas, que permiten la conexión a redes externas, este *firewall* está compuesto de dos dispositivos configurados en HA que garantizan que al fallar uno de estos dispositivos el otro sigue totalmente funcional con la misma configuración.	Se debe documentar todos los cambios que se realizan en el Core y generar una tarea (*checklist*) en la que se guarde el archivo de configuración antes de sacar el backup.
1.2.3	Instale *firewalls* de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos *firewalls* para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.	No existe	La empresa cuenta solo con un *firewall* perimetral configurado en alta disponibilidad que segmenta la red LAN a redes externas y DMZ. Las redes propagadas por los accesspoint dan alcance a la base de datos y aplicaciones que maneja los datos del titular y de la tarjeta.	Se debe instalar un *firewall* entre la red de Metlife y la red inalámbrica, segmentar la red donde se aloja la base de datos y aplicaciones CDE (entorno de datos del titular de la tarjeta) implementando por ejemplo ACLs, para que no pueda ser accedida por una persona malintencionada. Verificar que personal de la campaña Metlife que tiene acceso a la red inalámbrica solo se permita el tráfico necesario y permitido entre este dispositivo y el entorno de datos del titular de la tarjeta.
1.3	**Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.**	Inicial	El *firewall* está configurado para todo el tráfico hacia o desde internet o cualquier red externa esté debidamente controlada y autorizada desde las redes que gestionan los datos de los titulares de las tarjetas. No existe acceso al público a algún dato de datos del titular por ejemplo alojado en una DMZ. No existe un rol definido para el acceso a internet o redes externas a los analistas de calidad y estadística.	Garantizar que las redes internas que gestionan los datos de las tarjetas y titulares de las tarjetas tenga debidamente denegado o controlado el acceso a internet. Se debe definir y configurar a los analistas de calidad y estadística quienes tiene acceso a redes externas con mayores privilegios
1.3.1	Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos	Repetible	La compañía cuenta con un servidor DMZ el cual solo tiene publicado aplicaciones diferentes o que pertenecen a otro proceso o servicio de la compañía no a la campaña Metlife. Este DMZ está debidamente configurada con los puertos, servicios para que	Verificar que la configuración de las aplicaciones montadas en la DMZ estén con la debida documentación, gestión de cambios y análisis de riesgos.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	con acceso público autorizado.		solo se pueda ser accedida desde internet una aplicación o servicio particular	
1.3.2	Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.	Repetible	El servidor DMZ tiene configurados parámetros que bloquea servicios provenientes desde internet, solo está habilitado los puertos http y https	Generar procedimiento y debida documentación de la debida configuración de aplicaciones y configuraciones que debe terne el *firewall* relacionado al servidor DMZ
1.3.3	Implementar medidas anti suplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red.	Repetible	El *firewall* tiene configurado en sus políticas a conexiones de redes externas políticas de NAT que evitan que entes externos identifiquen que ips se manejan dentro de la compañía	Verificar que ninguna dirección ip interna sea visible a ninguna red. Verificar que en la reglas de DMZ tenga definida en sus reglas que las direcciones internas no se pueden transferir de Internet a la DMZ.
1.3.4	No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet	Inicial	Está definido el perfil de acceso de internet para los asesores y supervisores de la campaña., pero no está bien definido los perfiles para los analistas de calidad y estadística que tiene acceso a este.	Se debe bloquear o limitar el acceso a internet los analistas de estadística y de calidad, o cifrar la información u ocultar ciertos parámetros en las grabaciones para que este no tenga acceso a la información del titular de la tarjeta. Estas conexiones se deben inspeccionar con el fin de solo limitar el tráfico solo a las comunicaciones autorizadas.
1.3.5	Solo permita conexiones "establecidas" en la red.	Inicial	El *firewall* tiene configurado las conexiones entrantes a las redes internas de manera controlada, también hay configuradas acls a nivel LAN controlando el acceso de otras redes a la red que gestiona los datos del titular de la tarjeta. El *firewall* gestiona todos los *logs* de tráfico entrante y saliente.	Algunas políticas a intranets de los clientes no están bien definidas desde el origen, se debe especificar mejor estas políticas. Se sugiere documentar los perfiles y permisos específicos de las redes que tratan los datos del titular de la tarjeta.
1.3.6	Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.	Inicial	La red Interna (LAN) esta segregada de la red DMZ por medio de *firewall* y segmentada mediante ACL por el *SwitchCore*. No se guardan bases de datos en el servidor DMZ se alojan en un servidor interno y en un FTP otorgado por el cliente directamente.	Solicitar la cliente implementar parámetros de seguridad más confiable en el servicio FTP donde se aloja las bases de datos, documentar la estructura de red que evidencie como esta segregada la red de la compañía y todas las redes involucradas en el tratamiento de datos del titular de la tarjeta.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
1.3.7	No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.	Inicial	Todas la políticas de del *firewall* que dan conexión hacia internet tiene habilitado parámetros de NAT para que las redes internas no sean vistas desde internet	Generar documentación en la cual se establezcan requerimientos mínimos para establecer una política en el *firewall* que de acceso a internet tenga parámetros de NAT para evitar que las redes externas no sean visibles desde internet
1.4	**Instale *software* de *firewall* personal o una funcionalidad equivalente en todos los dispositivos móviles (de propiedad de la compañía y/o de los trabajadores) que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usan para acceder al CDE. Las configuraciones de *firewall* (o equivalente) incluyen: * Se definen los ajustes específicos de configuración. * El *firewall* personal (o funcionalidad equivalente) está en ejecución activa. * El *firewall* personal (o una funcionalidad equivalente) no es alterable por los usuarios de los dispositivos informáticos portátiles.**	No existe	Las políticas de *firewall* aplican en los dispositivos móviles mientras están dentro de las instalaciones de la compañía, cuando estos son usados externamente no cuentan con un *firewall* personal para limitar navegabilidad.	Se debe instalar un *firewall* personal a los equipos móviles corporativos como computadores portátiles, debe aplicar las políticas de seguridad y restricciones que se tiene dentro de las instalaciones de la compañía. El *firewall* personal no puede ser alterado por los usuarios de los dispositivos portátiles y siempre debe permanecer activo en cuanto el usuario final empiece a usar el equipo.
1.5	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los *firewalls* estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.**	Inicial	No se cuenta con documentación de las políticas de seguridad y administración del *firewall*. Se cuenta con procedimientos formales para solicitar permisos de acceso a redes externas.	Se debe documentar los procedimientos para realizar políticas de seguridad y conexiones redes externas y documentar el procedimiento para administrar los *firewall*'s. Se recomienda tomar como base la guía de la NIST-Guidelines on *Firewalls* and *Firewall Policy - Recommendations of the National Institute of Standards and Technology* - Karen Scarfone, Paul Hoffman

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
				Tener en cuenta aspectos como Políticas del *firewall* y Planificación e implementación.
Requisito 2	**No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.**			
2.1	**Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red.**	Inicial	La mayoría de servidores cuentan con usuarios y contraseñas establecidos por los administradores de las diferentes plataformas y estos no cuentan con cuentas predeterminadas, en cuanto al servidor NAS y los servidores de telefonía si cuentan con contraseñas establecidas por el proveedor, existe un FTP en el cual se suben y gestiona beses de datos que es otorgado directamente por el cliente, este también tiene un usuario y contraseña generado por el cliente y no se realiza cambio periódico del mismo. El servidor WSUS si cuenta con una cuenta predeterminada. El *firewall* cuanta con una usuario administrador por parte del proveedor para soporte, igualmente con los *switch* y el *Core*.	Los servidores de Telefonía y NAS debe tener una contraseña y usuario generadas por los administradores de plataforma de *Intercontact.* Solicitar al cliente que realice cambio periódico de contraseña en el FTP de manera periódica y que cumpla con requisitos mínimos para una contraseña segura. Deshabilitar o cambiar las contraseñas predeterminadas de los servidores NAS, de Telefonía y WSUS
2.1.1	En el caso de entornos inalámbricos que están conectados al entorno de datos del titular de la tarjeta o que transmiten datos del titular de la tarjeta, cambie TODOS los valores predeterminados proporcionados por los proveedores de tecnología inalámbrica al momento de la instalación, incluidas, a modo de ejemplo, las claves de cifrado inalámbricas predeterminadas, las contraseñas y las cadenas comunitarias	Inicial	Los *Acces point* o dispositivos que proporcionan conexión de red de manera inalámbrica, no tiene claves por defecto, el personal de la compañía que se conecta a estas redes y su dispositivo se conecta a este solo está permitido en equipos corporativos que son devueltos en el momento de su desvinculación, el personal transitorio o invitado que se conecta rara vez se conecta a una red de invitados que está totalmente aislada de la red interna mediante acls y cuya clave de acceso es cambiada semanalmente de manera automática. No se usan cadenas comunitarias SNMP	Documentar procedimiento sobre configuración de seguridad en los dispositivos de entornos inalámbricos (*Acces point*), que involucre cambio periódico de contraseña, sistema de cifrado, configuración de snmp, instalación, entre otros. Se debe generar la documentación de procedimientos que involucren parámetros de configuración de los *Acces point*, servidor de autenticación y actualización periódica de *firmware*. El *firmware* de los dispositivos se debe actualizar con cierto periodo de tiempo. Verificar que los *Acces point* no tengan valores

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	SNMP (protocolo simple de administración de red).		predeterminadas, la compañía usa SNMP llamado Nagios que fue configurado e instalado por el personal de tecnología de la compañía. No se usan contraseñas ni frase predeterminadas en los *Acces point*.	predeterminados proporcionados por el proveedor en ninguno de sus módulos o que los mismos hayan sido deshabilitados. Verificar que ningún dispositivo tenga configurado parámetros de cifrado débiles como WEP
2.2	**Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria.**	No existe	La compañía cuenta con procedimientos y políticas basados en la ISO27001-2013 pero no cuenta con normas de configuración de sistemas. La mayoría de los servidores de la compañía como son dominio, wsus, aplicaciones, pruebas, desarrollo, entre otros tiene configurados parámetros de *hardening* pero no se rige por ningún estándar en específico.	Crear documentación de procedimientos de configuración para los sistemas como servidores, *firewall*, *switch's*, etc. Estos procedimientos deben estar alineados con normas de seguridad como ISO, CIS, NIST, SANST. Toda esta documentación se debe actualizar a medida que se identifiquen nuevas vulnerabilidades en los sistemas que estén relacionado con la trazabilidad de los datos del titular de la tarjeta. Estos procedimientos de configuración deben ser implementados antes de la salida a producción de un sistema o nueva plataforma. Los procedimientos de configuración de estos sistemas deben incluir ciertos parámetros como: Cambiar valores y cuentas predeterminadas por el proveedor. Deshabilitar todas las funcionabilidades innecesarias. Implementar funciones seguridad adicionales para servicios que no se consideren seguros.
2.2.1	Implemente sólo una función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor.	Inicial	Algunos servidores no cuentan con un solo función principal por servidor, por ejemplo el servidor de dominio y el de antivirus están en el mismo servidor	Dado que existen varios servidores virtualizados en un solo servidor se debe inspeccionar las configuraciones del sistema y verifique que se haya implementado una sola función principal por componente de sistema o dispositivo virtual.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
2.2.2	Habilite solo los servicios, protocolos y *daemons*, etc., necesarios, según lo requiera la función del sistema.	Inicial	Se han realizado planes de trabajo de *hardening* en varios servidores con el fin de deshabilitar y controlar puertos, servicios, entre otros aspectos. Sin embargo, no existe un cronograma establecido para la ejecución frecuencia de estos planes de trabajo, y no se involucra todos los servidores de la compañía y que tienen relación directa con la campaña Metlife.	Implementar *hardening* en todos los servidores que tienen relación con la campaña metlife y estén involucrados con los datos del titular de la tarjeta, con el fin de garantizar que solo se ejecuten solo los servicios, *daemons*, puertos o protocolos necesarios. Todas estas normas de configuración deben ser debidamente documentadas con el fin de tener establecido todos los parámetros que deben ser deshabilitados o pueden estar permitidos en los diferentes servidores y equipos.
2.2.3	Implementar funciones de seguridad adicionales para los servicios, protocolos o *daemons* requeridos que no se consideren seguros.	No existe	Algunas servidores y aplicaciones utilizan parámetros o funciones no seguras como protocolos http, ftp, RDP, entre otros y no están documentados. Aunque las aplicaciones que involucran el ingreso de datos del titular y datos de la tarjeta son internas es decir solo son accedidas a nivel LAN, estas no utilizan protocolos de acceso seguro como TLS en una versión superior a 1.1. El servicio para alojar bases de datos de los clientes es un FTP que este mismo proporciono lo cual también es inseguro	Documentar las funciones y parámetros de seguridad que deben ser implementadas en todos los servicios y *daemons* no seguros. Configurar el servidor de aplicaciones y las aplicaciones relacionadas al uso de datos de titular de la tarjeta para que las aplicaciones antes de entrar a producción estas funcionen por tls 1.2 o superior. Solicitar al cliente la configuración segura del FTP como FTPS o SFTP según lo que el cliente Metlife se le facilite y asegure en mejor medida su información
2.2.4	Configure los parámetros de seguridad del sistema para evitar el uso indebido.	Inicial	Se configuran parámetros de seguridad pero no están documentados, ni existe una línea base de configuración de los mismos	Documentar normas con parámetros y valores de seguridad específicos para los componentes del sistema basarse en prácticas de hardening. Garantizar que los servidores, dispositivos y sistemas tengan configurados estos parámetros correctamente. Se pueden basar en parámetros de auditorías de sistemas como las que se muestra en libros como IT *Auditing using controls to protect information assets* (Chris Davis and Mike Schiller). Generar configuraciones en el *firewall* como A*ppplication Contol, Web Filters, políticas anti DDoS*, entre otros.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
2.2.5	Elimine todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.	Inicial	En los servidores, dispositivos y equipos tienen deshabilitados o eliminados parámetros que no se usan o no son necesarios para su debida funcionabilidad. No existe documentación con el fin de verificar que solo estén habilitadas ciertas funciones de manera segura No se han establecido parámetros específicos en seguridad del sistema.	Documentar los parámetros y valores específicos de seguridad que deben tener los servidores, equipos y dispositivos y que funciones o servicios debe estar habilitados de acuerdo al servidor. Configurar correctamente todos los sistemas con estos parámetros anteriormente documentados y establecidos.
2.3	**Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido.**	Inicial	Las aplicaciones que están relacionadas a la campaña metile en su administración no están configurados con un protocolo fuerte como ssl/tls. El *firewall*, el Core y switch su consola de administración es accedida por un protocolo seguro ssh por el puerto 2220. Los dispositivos de red y perimetrales tiene el puerto *telnet* deshabilitados	Configurar la administración de las aplicaciones con un protocolo seguro como tls mayor a 1.1. El acceso al servidor de aplicaciones debe utilizar un protocolo seguro con cifrado fuerte. Deshabilitar el acceso por http de la consola de administración y aplicaciones de la campaña Metlife. Se debe generar documentación que establezca el uso de criptografía fuerte en la administración basada en Web basada en las mejores prácticas de la industria. Por ejemplo la extensión de clave un mínimo de 112 bits de solidez y algoritmos de cifrado AES (128 bits y superior), TDES/TDEA (claves de triple extensión), RSA (2048 bits y superior), ECC (224 bits y superior) y DSA/D-H (2048/224 bits y superior).
2.4	**Lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS.**	Repetible	Existe un inventario de activos en los que se involucra campos como ID, procedimiento o área a la que pertenece, Nombre de activo, tipo, propietario, sede, estado y clasificación. El inventario de activos no se gestiona o actualiza con regularidad ni existe un campo donde describa la función o uso de cada componente.	Se debe involucrar en el inventario de activos existente todos los componentes relacionados con la campaña metlife y procesos que están involucrados en el tratamiento de los datos del titular de la tarjeta. Se debe incluir en el inventario de activos la descripción de la función o uso del activo. Generar una actualización periódica del inventario con una frecuencia definida o cuando ingrese o se cambie un activo existente.
2.5	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para**	Definido	Las políticas de seguridad de la compañía están documentadas, disponibles para todos los funcionarios de la compañía, existe una formación inicial en la	Realizar debidas mediciones con el fin de medir el desempeño de este control.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.		cual se capacita a todo el personal antes de su ingreso en las políticas de seguridad de la información. Las políticas son actualizadas o revisadas cada semestre.	
2.6	**Los proveedores de hosting compartido deben proteger el entorno y los datos del titular de la tarjeta que aloja la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el Anexo A1: Requisitos adicionales de las DSS de la PCI para los proveedores de servicios de *hosting.***	Definido	La compañía no cuenta con proveedores de hosting, el único hosting que existe es el correo electrónico, el cual es configurado mediante un oukloot en los equipos de cada funcionario, se generan políticas para el bloqueo de envío y recepción de correos que no tengan dominós corporativos. Se realizan informes del uso de correo electrónico mensualmente.	Ampliar el detalle de informes de la plataforma *google*, con el fin de monitorear otros aspectos como son *drive, docs.,* entre otros que ciertos perfiles tiene acceso.
Requisito 3	**Proteja los datos del titular de la tarjeta que fueron almacenados**			
3.1	**Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos que incluyan, al menos, las siguientes opciones para el almacenamiento de CHD (datos del titular de la tarjeta): Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio. Requisitos de retención específicos para datos de**	No existe	No se han generado políticas ni procedimientos que establezcan la limitación de almacenamiento de datos del titular de la tarjeta ni el tiempo de retención de los mismos. No se está establecido un proceso, ni políticas de retención para los datos de los titulares de la tarjeta que se tengan en cada uno de las áreas. Existe un procedimiento de borrado seguro en la compañía para medios removibles y estaciones de trabajo, pero este procedimiento de borrado seguro no cubre un proceso para identificar y eliminar de manera segura los datos del titular de la tarjeta que hay cumplido su tiempo de retención definida con anterioridad. No se tiene establecido un procedimiento que defina donde se deben o se están guardando estos datos del titular. Los lugares donde se alojan los datos del titular son el servidor	Establecer una reunión con el cliente Metlife para determinar y generar un procedimiento y políticas para la limitación de almacenamiento de datos del titular de la tarjeta y retención de los mismos de acuerdo a requisitos legales, reglamentarios y del negocio. Se debe establecer un proceso de eliminación segura de datos del titular de la tarjeta cuando estos ya no son necesarios por motivos legales, temas contractuales o reglamentarios basándose en el proceso de borrado seguro que existe actualmente en la compañía. Se deben realizar auditorías o revisiones con el fin de identificar por lo menos trimestralmente para identificar y eliminar de manera segura estos datos anteriormente nombrados y que cumplan los requisitos de

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	titulares de tarjetas. Procesos para eliminar datos de manera cuando ya no se necesiten. Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan la retención definida.		de aplicaciones, bases de datos, ftp del cliente, grabaciones telefónicas. En la compañía se almacenan datos del titular como son el PAN, fecha de vencimiento, tipo (mastercard, visa), datos personales como nombres, facha de nacimiento, cédula, correo electrónico, nombres de afiliados y dirección.	retención estipulados se debe cubrir todos los lugares donde se almacenan los datos del titular. Se deben crear procesos de retención y eliminación de datos que debe cubrir todos los lugares donde se almacenan estos, entre los datos deben estar nombres del titular de la tarjeta. Verificar que datos realmente son necesarios almacenar para el debido funcionamiento de la campaña Metlife.
3.2	**No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos de autenticación confidenciales, convierta todos los datos en irrecuperables al finalizar el proceso de autorización.**	Inicial	La compañía no almacena datos confidenciales de autenticación, solo toma los números de la cuenta principal (PAN), nombre del titular de la tarjeta, y fecha de vencimiento. En el momento no existe una razón legítima para realizar retención de datos confidenciales de las tarjetas de pago.	Aunque la compañía no almacene, ni trate datos confidenciales de autenticación, documentar en un procedimiento o política que este tipo de procedimiento no se realiza por la compaña y en caso de realizarse en un futuro cómo se gestiona la debida eliminación y no almacenamiento de los mismos para que sean irrecuperables.
3.2.1	No almacene contenido completo de ninguna pista (de la banda magnética ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo) después de la autorización. Estos datos se denominan alternativamente, pista completa, pista, pista 1, pista 2 y datos de banda magnética.	Inicial	La campaña Metlife almacena datos del titular de la tarjeta como: Número de cuenta principal Fecha de vencimiento Nombre del titular de la tarjeta Tipo (visa, Mastercard) No se guardan contenidos completos de ninguna pista.	Se debe establecer políticas que indiquen cuales son los únicos valores que pueden ser almacenados en los cuales no puede ser involucrados el contenido completo de ninguna pista. Para identificar que datos del titular de la tarjeta son almacenados se recomienda realizar una búsqueda automatizada con herramientas free como Cardito, CCSRCH, Find_SSNs, OpenDLP, Spider, entre otras.
3.2.2	No almacene el valor o código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago que se utiliza para verificar las transacciones de tarjetas ausentes) después de la autorización.	Inicial	En la campaña metlife no se almacena el valor o código de validación de tarjetas. Ni realiza procedimientos de transaccionalidad.	Se debe establecer políticas que indiquen cuales son los únicos valores que pueden ser almacenados en los cuales no puede ser involucrado como el valor o código de validación de tarjetas.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
3.2.3	Después de la autorización, no almacene el PIN (número de identificación personal) ni el bloqueo de PIN cifrado.	Inicial	En la campaña metlife no se almacena, ni se solicita el PIN al titular de la tarjeta	Se debe establecer políticas que indiquen cuales son los únicos valores que pueden ser almacenados o solicitados en los cuales no puede estar involucrado el PIN
3.3	**Enmascare el PAN (número de cuenta principal) cuando aparezca (los primeros seis o los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis o los últimos cuatro dígitos del PAN.**	No existe	No están estipulados en ningún procedimiento las funciones o perfiles que deben tener acceso a todo el número PAN. Todos los funcionarios que están involucrados en la manipulación y acceso en los datos del titular tienen acceso a todo el número PAN.	Generar un documento que estipule las funciones o perfiles que están específicamente autorizadas para ver el número PAN completo. Enmascarar u ocultar los seis o los últimos cuatro dígitos del PAN de modo que sea solo legibles para los perfiles específicos y definidos legalmente por una necesidad comercial Implementar procedimientos y configuraciones del sistema para que la visualización del PAN solo sea permitidos a funciones o perfiles específicos o enmascarar el PAN y dejar solo los últimos dígitos para realizar una función comercial.
3.4	**Convierta el PAN (número de cuenta principal) en ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros)**	No existe	Los números PAN son almacenados de manera legible en la totalidad del número en las bases de datos, aplicaciones, servicio FTP y puede ser escuchado en su totalidad en las grabaciones de la planta telefónica.	Convertir el número PAN en ilegible para su debido almacenamiento utilizando técnicas como hash, truncamientos, *tokens* y criptografía sólida. Implementar un procedimiento donde se establezca un sistema para proteger el PAN utilizando algún sistema como *hash*, truncamiento, *token* o criptografía sólida. Todos los números PAN deben estar protegidos sin importar su lugar de almacenamiento.
3.4.1	Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales	No existe	Las grabaciones en las cuales se registran las ventas efectivas de Metlife y cuentan con los datos del titular de la tarjeta como es el número PAN, fecha de vencimiento de la tarjeta, datos personales del cliente, etc. Son enviados al cliente por medio de un CD cuya información es comprimida y cifrada por un algoritmo de cifrado AES256, en cuanto la clave de descifrado es enviada por correo electrónico directamente al cliente que va auditar las llamadas. El cifrado de discos solo es	Cifrar la base de datos que están SQL con un cifrado seguro como AES 256, dado la base de datos SQL es superior a 2006 este se puede cifrar con ciertos parámetros de manera simétrica o asimétrica, para el entono de la compañía es recomendable simétrico. las recomendaciones se pueden observar en el siguiente link https://msdn.microsoft.com/es-es/library/ms188357.aspx

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con las cuentas de usuarios.		utilizado en algunos equipos portátiles. Las bases de datos no se cifran	
3.5	**Documente e implemente procedimientos que protejan las claves utilizadas para proteger los datos del titular de la tarjeta almacenados contra su posible divulgación o uso indebido**	Inicial	Los datos del titular de la tarjeta son almacenados en los siguientes ambientes: En una la base de datos alojada en el servidor de aplicaciones. Almacenados en las grabaciones las cuales son alojadas en el servidor de telefonía. Mediante una VPN que es otorgada por el cliente, Mediante un FTP proporcionado por el cliente también se aloja información del titular de la tarjeta. Mensualmente se envía un CD cifrado con las grabaciones de las ventas efectivas. Todos estos ambientes son utilizan información tanto de la tarjeta como número PAN, fecha de vencimiento, franquicia, como datos personales del titular de la tarjeta. Todos estos datos son manipulados por varios funcionarios y áreas de la compañía. No existe ningún tipo de procedimiento documentado en el que se establezca como se debe proteger esta información. La base de datos alojada en el servidor de aplicaciones si está protegida contra lectura, escritura y modificación. Los asesores solo pueden ingresar datos mas no lo pueden consultar o modificar. Los perfiles para auditar las llamadas están configurados para que solo el analista de calidad pueda escuchar las grabaciones respectivas, el ingreso es por medio de usuario y contraseña. Los aplicativos de VPN y FTP otorgados por el cliente son administrados por ellos, cabe notar que los perfiles en el FTP no está muy bien definidos y las claves e usuarios no se cambian con periodicidad. La clave para descifrar los archivos guardados en el CD	Se debe establecer procedimientos y políticas para la protección de contraseñas que son usadas para la protección de datos del titular en todos sus ambientes (bases de datos, aplicaciones, cifrado de cd´s, almacenamiento de grabaciones, etc.). Este procedimiento debe involucrar aspectos como son: Limitar al menor número posible de custodios de las claves. Características de las claves de cifrado para cifrar estas claves. *Almacenamiento que debe ser en la menor cantidad de ubicaciones y formas posibles. Establecer protocolos de seguridad con el cliente Metlife para reforzar el acceso a la VPN y el FTP y custodiar las claves de acceso de acuerdo al procedimiento y políticas establecidas.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
			que se envía al cliente se envían directamente al cliente por medio de correo electrónico. La compañía actualmente cuanta con un procedimiento de gestión de claves donde se establecen parámetros mínimos para asignar contraseñas seguras.	
3.5.1	Requisitos adicionales solo para los proveedores de servicios: Mantenga una descripción documentada de la arquitectura criptográfica que incluye: Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos del titular de la tarjeta, incluidas la complejidad de la clave y la fecha de caducidad. Descripción del uso de la clave para cada tecla. Inventario de un HSM SMS y otros SCD utilizados para la gestión de claves	No existe	No existe documentación relacionada con los algoritmos de encripción usados para cifrar por ejemplo las grabaciones. No se cifra la base de datos ni se utiliza métodos seguros para en envió de transporte por el FTP	Cifrar la información alojada en la base de datos, también utilizar un protocolo seguro en vez de utilizar solo FTP, documentar que algoritmos de cifrado se están o se van a usar.
3.5.2	Restrinja el acceso a las claves criptográficas a la menor cantidad de custodios necesarios	No existe	No existe un procedimiento, ni políticas que establezcan cuales son las claves criptográficas que se usan y a quien se deben restringir. En la actualidad la única clave que se usa para cifrar datos del titular de la tarjeta es la que se usa para cifrar el CD con grabaciones. Los otros entornos que manipulan datos del titular de la tarjeta no están cifrados y las contraseñas usadas no están cifradas. La información de la clave del cifrado del CD solo es de conocimiento del líder de calidad y el cliente de metlife.	Cifrar la información que debe ser cifrada de los datos del titular y las claves de cifrado de estas bases debe ser debidamente cifradas y restringidas al personal definido. Esto debe ser regido de acuerdo a unos procedimientos y políticas establecidas, así como los dispositivos que generan, utilizan y protegen las claves. Cifrar las bases de datos que contiene la información de los datos del titular con un cifrado fuerte como AES256, la claves de cifrado deben ser debidamente custodiadas por un personal designado. Cifrar el número PAN y los demás datos considerados como confidenciales.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
3.5.3	Siempre guarde las claves secretas y privadas utilizadas para cifrar/descifrar los datos del titular de la tarjeta en una (o más) de las siguientes formas: Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de *host]* o un dispositivo de punto de interacción aprobado para la PTS). Como, al menos, dos claves o componentes de la clave completos de acuerdo con los métodos aceptados por la industria	No existe	No existe ningún método para guardar las claves secretas, dado que en la actualidad ni siquiera se cifra los datos del titular de la tarjeta	Cuando se empiece a cifrar y a descifrar los datos del titular de la tarjeta, se debe utilizar técnicas para guardar estas claves con que se cifra o descifra con métodos como usar una clave de cifrado al menos tan sólida como la clave de cifrado de datos, utilizar un dispositivo criptográfico HSM, un dispositivo de punto de interacción aprobado para la PTS.
3.5.4	Guarde las claves criptográficas en la menor cantidad de ubicaciones posibles.	No existe	No existe ningún método para guardar las claves secretas, dado que en la actualidad ni siquiera se cifra los datos del titular de la tarjeta	Cuando se empiece a cifrar y a descifrar los datos del titular de la tarjeta, se debe almacenar las claves de cifrado en la menor cantidad de sitios posibles
3.6	**Documente por completo e implemente todos los procesos y procedimientos de administración de claves de las claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta,**	No existe	No existe un procedimiento que determine los procedimientos de administración de claves entre el cliente Metlife y la compañía Intercontact. Ninguna de estas claves está cifradas. De igual manera los datos del del titular de la tarjeta que son manejados entre los aplicativos del cliente con Intercontact no son cifrados. Existe unas políticas de claves en Intercontact	Se deben crear unos procedimientos para cifrar la información del titular de la tarjeta y administración de claves utilizadas para cifrar esta información. El método de envió de datos por medio del FTP debe involucrar métodos seguros para el envió de información con SFTP y SFTP, la calve de acceso de FTP debe terne un debido custodio, y esta debe ser cambiada con regularidad. Los parámetros de VPN utilizados deben generar también un cambio periódico de contraseña.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
3.6.1	Generación de claves de cifrado sólido	No existe	No existe un procedimiento para el ciframiento de datos de los titulares de la tarjeta	Cuando se implemente el ciframiento de los datos del titular da la tarjeta se debe generar el procedimiento de generación de claves de cifrado que debe especificar como generar claves sólidas, de acuerdo a estándares como NIST *Special Publication* 800-133, ISO 11568-2 Servicios financieros, ISO 11568-4 Servicios financieros
3.6.2	Distribución segura de claves de cifrado	No existe	No existe un procedimiento para el ciframiento de datos de los titulares de la tarjeta	Cuando se implemente el ciframiento de los datos del titular da la tarjeta se debe generar el procedimiento de generación de claves en el cual se debe involucrar aspectos que especifiquen la distribución de claves de manera segura en los cuales involucre aspectos como que solo se distribuyan a las personas específicas y nunca se haga en texto claro.
3.6.3	Almacenamiento seguro de claves de cifrado	No existe	No existe un procedimiento para el ciframiento de datos de los titulares de la tarjeta	Cuando se implemente el ciframiento de los datos del titular da la tarjeta, las claves de cifrado utilizadas se deben guardar de manera segura.
3.6.4	La clave criptográfica cambia en el caso de las claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que cierta cantidad de texto cifrado haya sido producido por una clave dada), según lo defina el proveedor de la aplicación relacionada o el responsable de las claves, y basándose en las mejores prácticas y recomendaciones de la industria	No existe	No existe un procedimiento para el ciframiento de datos de los titulares de la tarjeta	Cuando se implemente el ciframiento de los datos del titular da la tarjeta, determinar un periodo de uso de claves para el uso de la misma durante un periodo definido.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
3.6.5	Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción o revocación) según se considere necesario cuando se haya debilitado la integridad de la clave (por ejemplo, salida de la empresa de un empleado con conocimiento de una clave en texto claro, etc.) o cuando se sospeche que las claves están en riesgo.	No existe	No existe un procedimiento para el ciframeinto de datos de los titulares de la tarjeta	Involucrar en los procedimientos de gestión de claves el retiro o remplazo de claves cuando se presente casos como retiro o remplazo de claves, remplazo de claves cuando se sospechen que están en riesgo y cuando un empleado es retirado de la compañía y conoce la clave.
3.6.6	Si se usan operaciones manuales de administración de claves criptográficas de texto claro, se deben realizar con control doble y conocimiento dividido.	No existe	No se utilizan claves seguras, ni tampoco un método seguro en el envió de información por el FTP, las contraseñas usadas para el envió de información mediante el CD muchas veces no cumplen parámetros de seguridad y esta clave solo está en el conocimiento de un solo funcionario de la compañía.	Configurar un método seguro para en envió de información mediante el FTP, puede ser métodos SFTP o FTPS, la clave para acceder a este aplicativo debe ser conocimiento compartido así solo lo use una persona. El cifrado utilizado debe ser simétrico con el fin que tanto el receptor como emisor conozcan la clave. Cuando se envié los datos de grabaciones cifradas en un CD la contraseña no solo puede estar en conocimiento a un solo funcionario de la compañía, el conocimiento debe ser compartido, las claves de cifrado deben ser seguras utilizando parámetros de seguridad como alfanuméricos, mayúsculas, minúsculas, números y mínimo 8 caracteres
3.6.7	Prevención de sustitución no autorizada de claves criptográficas.	No existe	Los procedimientos de gestión de claves no involucran aspectos como procesos para evitar la sustitución no autorizada de claves.	Involucrar en el procedimiento de gestión de claves aspectos que especifiquen actividades prevenir la sustituciones de claves sin el debido permiso.
3.6.8	Requisito para que los custodios de claves criptográficas declaren, formalmente, que comprenden y aceptan su responsabilidad como custodios de claves.	No existe	No existe un procedimiento de custodia de claves criptográficas	Involucrar en los procedimientos de gestión de claves los formatos en los cuales se establece la responsabilidad de los custodios donde aceptan y comprenden su responsabilidad como custodios de claves.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
3.7	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.**	Inicial	Existen políticas de seguridad de la información en las cuales se pueden nombrar las siguientes relacionadas con la protección de la información como políticas sobre uso aceptable de los activos, política de control de acceso a la información y política de tratamiento de datos personales, no existen políticas de seguridad que establezcan específicamente la debida protección de los datos del titular. Las políticas anteriormente nombradas están publicadas, son de conocimiento por todos los integrantes de la compañía y están son informadas en un proceso de formación inicial	Completar las políticas de seguridad de la información con aspectos detallados sobre la protección de datos del titular de la tarjeta y que esto sean de conocimiento a los funcionarios de la compañía.
Requisito 4	**Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas**			
4.1	**Utilizar criptografía sólida y protocolos de seguridad para proteger los datos del titular de la tarjeta confidenciales durante la transmisión por redes públicas abiertas, como por ejemplo, las siguientes:** **Solo se aceptan claves y certificados de confianza.** **El protocolo implementado solo admite configuraciones o versiones seguras.** **La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza**	Inicial	Las aplicaciones internas que utilizan los asesores para recolectar los datos del titular de la tarjeta utilizan un protocolo TLS1.0 pero esta aplicación solo es posible ser accedida de manera local. Con redes externas se tiene configurado un ftp proveído por el cliente, este aplicativo no es seguro. Se cuenta también con una VPN con el cliente la cual si cuenta con un cifrado seguro e instalado en un equipo definido para acceder a la misma. No se recibe o transmiten de otra manera los datos del titular de la tarjeta y datos de la tarjeta. No existe documentación que establezca las configuraciones que deben tener los sistemas como son las aplicaciones, el aplicativo ftp y la vpn s*ite to client* que se tiene con el cliente. No existe documentación que establezca que:	El servidor FTP que se tiene para alojar y descargar información debe tener una configuración de seguridad adecuada, debe utilizar un protocolo seguro, además de crear perfiles concretos para cada usuario y cambio periódico de contraseña. Se debe establecer en conjunto con el cliente un servicio en FTPS o SFTP según sea lo más conveniente y fácil para el cliente. Se debe documentar políticas y procedimientos que establezca la configuración segura para el transporte seguro de información con claves, certificados de confianza, que solo se acepte versiones y configuraciones seguras y cifrado sólido. Se debe configurar la aplicación Web que se usa a nivel LAN con https y habilitar TLS 1.2 o superior al trasmitir o recibir los datos del titular de la tarjeta.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
4.1.1	Asegúrese de que las redes inalámbricas que transmiten los datos del titular de la tarjeta o que están conectadas al entorno de datos del titular de la tarjeta utilicen las mejores prácticas de la industria a fin de implementar un cifrado sólido para la transmisión y la autenticación.	Repetible	En la compañía existen dos tipos de redes inalámbricas, una en la cual se conecta solo los funcionarios de la compañía que tiene asociada su dirección Mac y otra red para invitados que está aislada de la red LAN de la compañía. El cifrado de transmisión de la red inalámbrica es WPA2. Aunque la aplicación que maneja los datos del titular de la tarjeta puede ser accedida desde un equipo móvil como un portátil, ninguno de los equipos que utilizan esta aplicación son dispositivos móviles. Existen políticas de seguridad de la información la cual establece que solo el personal que esté debidamente autorizado y trabaje para la compañía se puede conectar a la red inalámbrica corporativa.	Genere la debida documentación y procedimientos para el debido acceso y configuración de un equipo a las red inalámbrica corporativa, de igual manera establecer documentalmente el tipo de protocolo uy mejores proactivas de seguridad de la industria que deben tener configurados los *Acces point.* Configurar para que los *Access point* solo puedan ser accedido de manera segura por protocolos como https.
4.2	**Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, SMS, el chat, etc.)**	No existe	No se cifra en ningún momento el número PAN, en la trasmisión de este mediante el ftp con el cliente, ni con el aplicativo web interno que se usa, este número no se envía cifrado o de manera ilegible. En los procesos de la campaña no se utiliza medios de tecnologías de usuario final para enviar números PAN	Cifrar el numero PAN en las transmisiones de este por el FTP o el aplicativo web, se debe establecer políticas que establezcan que los PAN no protegidos no se deben enviar por medio de tecnología de usuario final
4.3	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.**	No existe	No existe documentación relacionada a políticas de seguridad, procedimientos para cifrar las transmisiones de datos del titular de la tarjeta	Se debe implementar procedimientos y políticas que establezcan que los datos del titular de la tarjeta sean cifrados en las transmisiones y que estos sean documentados, estén en uso y sean de conocimiento para todas las partes interesadas.
Requisito 5	**Proteger todos los sistemas contra *malware* y actualizar los programas o *software* antivirus regularmente**			

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
5.1	**Implemente un *software* antivirus en todos los sistemas que, generalmente, se ven afectados por *software* malicioso (en especial, computadoras personales y servidores).**	Definido	Todos los computadores de la compañía tiene instalado antivirus, también los servidores tiene agente de antivirus. El servidor de antivirus esta actualizado y los agentes son actualizados con frecuencia, se generan informes semanales de la consola de antivirus.	Evaluar el desempeño de la consola de antivirus ejerce sobre los equipos y servidores.
5.1.1	Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de *software* malicioso conocidos y proteger a los sistemas contra estos.	Definido	La consola de antivirus detecta cierto varios tipos de *malware* y ataques como *phishing*. Esta consola también elimina *malware* o los almacena en cuarentena algún tipo de *software* desconocido o no confiable.	Evaluar el desempeño de la consola de antivirus ejerce sobre los equipos y servidores.
5.1.2	Para aquellos sistemas que no suelen verse afectados por *software* maliciosos, lleve a cabo evaluaciones periódicas para identificar y evaluar las amenazas de *malware* que pueden aparecer a fin de determinar si es necesario o no implementar un *software* antivirus en dichos sistemas.	Inicial	Los servidores de telefonía no tiene instalado *software* de antivirus, ya que el acceso a internet es muy limitado, de igual manera se debe verificar su instalación dado que información del titular de la tarjeta es guardada allí mediante grabaciones.	Aunque los servidores de telefonía tienen acceso limitado a internet, se debe evaluar que estos sistemas no se vean afectados por ningún tipo de *malware*
5.2	**Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: Estén actualizados. Ejecuten análisis periódicos. Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS**	Repetible	La consola de antivirus se mantiene actualizada consultando servidores alojados en internet, esta consola de antivirus actualiza todos los días los agentes *endpoint* instalados en cada uno de los equipos y servidores de la compañía. Los análisis periódicos no están muy bien definidos, de igual manera se generan informes semanales de la consola de antivirus	Definir la periodicidad para la ejecución de análisis en los equipos y servidores de la compañía. Documentar en las políticas existentes indicando que el antivirus debe realizar actualizaciones automáticas. Verificar que este configurado en la consola de antivirus la ejecución de análisis periódicos y documentar la periodicidad del mismo. Se debe conservar los registros de auditoria.
5.3	**Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y**	Definido	Por políticas de directorio activo ningún equipo puede deshabilitar, alterar o desinstalar el agente de antivirus instalado en el *host*, este es ejecutado permanentemente. Este tipo de privilegio solo es posible con una cuenta administradora	Definir procedimientos documentados que establezcan las actividades que se deben llevar a cabo cuando es necesario desactivar la protección del antivirus, por ejemplo deshabilitar el acceso a internet y realizar un análisis completo cuando este se vuelva a habilitar.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	durante un período limitado.			
5.4	**Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.**	Definido	La compañía cuenta con política de antivirus que es conocida por todas las partes y puede ser consultada	Se debe ejecutar actividades que evalúen el desempeño del control con el fin de garantizar el correcto cumplimento del mismo.
Requisito 6	**Desarrollar y mantener sistemas y aplicaciones seguros**			
6.1	**Establezca un proceso para identificar las vulnerabilidades de seguridad por medio de fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad, y asigne una clasificación de riesgo (por ejemplo, "alto", "medio" o "bajo") a las vulnerabilidades de seguridad recientemente descubiertas.**	Definido	Se realiza análisis de vulnerabilidades de manera semestral a la infraestructura tecnológica y revisiones de seguridad de las aplicaciones antes que estas salgan a producción utilizando programas de la OWASP, entre otros. Los análisis de vulnerabilidades se realizan con herramientas de análisis de vulnerabilidades como *Nessus, OpenVass, Nexpose*, entre otros que basan su riesgo de factor en CVSS. La criticidad de las vulnerabilidades se basa en la calificación CVSS que asigna la herramienta de análisis de vulnerabilidades con un análisis de contexto de la empresa. Existen indicadores relacionados a la solución de vulnerabilidades de manera oportuna, asignando la solución de vulnerabilidades en alto 15 días, medias 45 días y bajas en 60 días. Las vulnerabilidades se asignan a determinados riesgos de la infraestructura tecnológica de la empresa, sobre todo las vulnerabilidades clasificadas en críticas, altas y medias.	Dado que el análisis de vulnerabilidades que se realiza es a nivel interno, se requiere se revisen ciertos criterios para la evaluación de las vulnerabilidades y asignar la clasificación de riesgo a esas vulnerabilidades basándose en un proceso que controle activamente las fuentes de la industria para obtener información sobre las vulnerabilidades https://www.pcihispano.com/criterios-para-escoger-un-proveedor-aprobado-de-escaneo-asv/

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
6.2	**Asegúrese de que todos los *software* y componentes del sistema tengan instalados parches de seguridad proporcionados por los proveedores que ofrecen protección contra vulnerabilidades conocidas. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento.**	Definido	Se cuenta con la plataforma WSUS con el fin de instalar automáticamente y de manera controlada los parches de seguridad en equipos y servidores.	No existen políticas establecidas sobre la instalación de parches de seguridad en los equipos, solo se cuenta con mantenimientos periódicos en la instalación de parches en servidores. La instalación de parches críticos aun esta desactualizada de acuerdo al mes de publicación de los parches. Se deben establecer tiempos máximos para la instalación de parches, de acuerdo a las políticas, la instalación de parches de criticidad alta deben ser instalados por ejemplo cada mes. No se tiene gestionado correctamente la instalación de parches de manera periódica a los sistemas operativos que no son *Windows*.
6.3	**Desarrolle aplicaciones de *software* internas y externas (incluso acceso administrativo a aplicaciones basado en web) de manera segura y de la siguiente manera: De acuerdo con las PCI DSS (por ejemplo, autenticación y registros seguros). Basadas en las normas o en las mejores prácticas de la industria. Incorporación de seguridad de la información durante todo el ciclo de vida del desarrollo del *software*.**	Inicial	Cuando se realiza desarrollo *software in-house*, en su estado de pruebas se realizan verificaciones de seguridad y se exige unos requerimientos de seguridad mínimos como son autenticación, contraseña fuerte, deslogueo automático de sesiones, cumplimiento con parámetro de seguridad como es el top 10 de la OWASP.	No se gestionan *logs* de auditoria de las aplicaciones, se debe involucrar formalmente la seguridad de la información durante todo el ciclo de vida del *software* en los requisitos, el diseño, el análisis y las fases de prueba de desarrollo, por ejemplo estableciéndolo en el flujo grama del proceso, o la política de desarrollo estos aspectos. Revisar el proceso de desarrollo, para involucrar actividades de desarrollo seguro como el libro de la OWASP A *Guide to Building Secure Web Applications and Web Services - 2.0 Black Hat Edition,* también el libro *Software Security Building Security in* Gary McGraw - Addison-Wesley
6.3.1	Elimine las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas antes de que las aplicaciones se activen o se pongan a disposición de los clientes.	Inicial	A nivel documental no está establecido que los ID de usuarios y las contraseñas utilizadas en los ambientes de prueba se eliminen antes de enviar la aplicación a producción. De igual manera se utiliza una base de datos de pruebas que no es utilizada en producción.	Se debe documentar a nivel procedimental en el proceso de desarrollo de aplicaciones la eliminación de los ID de usuarios y contraseñas utilizadas en los ambientes de prueba antes que estas salgan a producción.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
6.3.2	Revise el código personalizado antes de enviarlo a producción o de ponerlo a disposición de los clientes a fin de identificar posibles vulnerabilidades en la codificación (mediante procesos manuales o automáticos) y que incluya, al menos, lo siguiente: La revisión de los cambios en los códigos está a cargo de personas que no hayan creado el código y que tengan conocimiento de técnicas de revisión de código y prácticas de codificación segura. Las revisiones de los códigos deben garantizar que el código se desarrolle de acuerdo con las directrices de codificación segura. Las correcciones pertinentes se implementan antes del lanzamiento. La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento.	Inicial	Se realiza validaciones de seguridad por parte del oficial de seguridad informático de la compañía. Existe comité de cambios, las aplicaciones antes de salir a producción deben ser aprobadas, pero en ocasiones las pruebas de seguridad y aprobaciones no se realizan antes de su salida a producción. La revisión en los cambios de código es realizada por la misma persona que realiza el código. No está establecido un procedimiento o estructura formal a seguir para el desarrollo o codificación segura de aplicaciones.	Todos las aplicaciones que van a salir a producción deben ser aprobadas por el comité de cambios o en su defecto por la gerencia, de igual manera las pruebas de seguridad deben ser realizadas antes de su salida a producción. Se debe asignar una persona distinta al desarrollador para realizar las revisiones de código cuando se generen cambios en estos, esta persona debe tener conocimientos en técnicas de revisan de código. Se debe generar un procedimiento o estructura formal para realizar un desarrollo seguro, las revisiones de código deben garantizar que el desarrollo cumpla con esta estructura. Se puede usar prácticas de codificación segura de la OWASP.
6.4	**Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema.**	Definido	Existe un procedimiento de gestión de cambios en componentes de infraestructura y una política de adquisición, desarrollo y mantenimiento de *software*. Los entornos de pruebas y desarrollo están separados tanto en ambientes equipos como vlans o redes, se tiene implementado un control de acceso para el ingreso a los servidores. Está definido que los procesos de desarrollo, pruebas y producción están separados pero solo una persona ejerce en los tres ambientes. Los datos del numero PAN no se usa en los ambientes de desarrollo ni pruebas, en estos	El funcionario encargado para realizar el proceso de desarrollo y pruebas, debe ser distinto del que configura la aplicación al ambiente de producción. Se debe cumplir lo que está documentado en el procedimiento y en la política de adquisición, mantenimiento y desarrollo de *software*. Incluir en el procedimiento de desarrollo la eliminación formal de las cuentas de pruebas antes de que la aplicación salga a producción. Siempre que se vayan a realizar cambios a nivel de *software*, implementaciones de nuevas aplicaciones están deben ser aprobadas por el comité de cambios antes de su

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
			ambientes se utilizan bases de datos de prueba.	salida a producción. Dentro del procedimiento de control de cambios debe estar relacionado que se hayan realizado las pruebas de seguridad con anterioridad.
6.4.1	Separe los entornos de desarrollo/prueba de los entornos de producción y refuerce la separación con controles de acceso.	Definido	Los ambientes de pruebas y desarrollo están separados del ambiente de producción, el proceso se realiza en servidores diferentes y redes diferentes. A estos servidores tiene acceso el desarrollador, aunque en el servidor de producción el desarrollador solo tiene acceso a una carpeta que es donde se aloja las aplicaciones, estos permisos deben ser bloqueados.	El desarrollador solo debe tener acceso a los ambientes de desarrollo y pruebas, la aplicación debe ser aplicada a producción por un funcionario distinto. Se debe bloquear el acceso al desarrollador al ambiente de producción. Igualmente se debe bloquear el acceso a la base de datos de producción al desarrollador.
6.4.2	Separación de funciones entre desarrollo/prueba y entornos de producción	Inicial	Aunque a nivel documental tanto en el procedimiento como en las políticas los ambientes de desarrollo, pruebas y producción están separados, el desarrollador de la compañía está encargado de realizar el desarrollo, realizar las pruebas y subir el aplicativo al ambiente de producción.	Se debe designar, y asignar funciones a un cargo del proceso de tecnología que involucren la configuración de las aplicaciones que van a salir a producción.
6.4.3	Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo	Inicial	Los datos de producción PAN activos no se utilizan en los ambientes de desarrollo y pruebas, se utiliza bases de datos de pruebas.	Incluir en el procedimiento de manera formal que los datos que están en producción no pueden ser utilizados en los ambientes de pruebas ni desarrollo.
6.4.4	Eliminación de datos y cuentas de los componentes del sistema antes de que se activen los sistemas de producción	No existe	Aunque se observa que se utiliza datos ficticios en los ambientes de pruebas y desarrollo, no se evidencia ningún procedimiento formal establecido en el cual se eliminen todas estas cuentas utilizadas en estos ambientes.	Se debe involucrar en el procedimiento de desarrollo que se eliminen los datos y cuentas de los componentes del sistemas antes de que estos salgan al ambiente de producción
6.4.5	Los procedimientos de control de cambios	Inicial	Aunque existe un procedimiento de gestión de cambios establecido por INTERCONTACT, este no cumple con parámetros específicos cuando se deben realizar cambios a nivel de aplicaciones por alguna incidencia, o cambio solicitado por el cliente.	Complementar el procedimiento de gestión de cambios con aspectos como la documentación de la incidencia, aprobación del cambio por las partes autorizadas, pruebas de funcionabilidad y procedimientos de desinstalación.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
6.4.5.1	Documentación de incidencia	No existe	No existe una documentación de incidencia, solo existe un requerimiento por parte de los clientes.	Se debe involucrar en el documento de gestión de cambios, la documentación de la incidencia que genero el cambio o actualización en la aplicación. También se debe documentar el impacto del cambio.
6.4.5.2	Aprobación de cambio documentada por las partes autorizadas.	Inicial	En el comité de cambios se aprueba los respectivos cambios que se van a realizar en la aplicación.	Se debe documentar que los cambios también son autorizados por el cliente, en la actualidad en las partes interesadas si se informa al cliente cuando el cambio es a nivel de infraestructura pero no a nivel de aplicaciones.
6.4.5.3	Verifique que se hayan realizado las pruebas de funcionalidad y que el cambio no impacte negativamente en la seguridad del sistema.	Definido	Se realizan pruebas de funcionabilidad cuando se realizan cambios en las aplicaciones, de igual manera pruebas de seguridad en los sistemas	Se deben estipular un número de pruebas más rigurosas sobre el sistema, para verificar que el entrono no se reduce al implementar el cambio y que los controles de seguridad antiguamente instalados no hayan desmejorado en su efectividad o se remplacen por controles igualmente sólidos.
6.4.5.4	Procedimientos de desinstalación	No existe	No existe un proceso de desinstalación cada vez que se realiza un cambio en alguna aplicación.	Se debe documentar un proceso de desinstalación cada vez que se realiza un cambio en una aplicación, para permitir devolver cambios en caso que el cambio falle o la seguridad en el sistema aplicación sea afectada.
6.4.6	Al término de un cambio significativo, deben implementarse todos los requisitos pertinentes de la PCI DSS en todos los sistemas y redes nuevos o modificados, y la documentación actualizada según sea el caso.	Inicial	Los cambios que se realizan en términos de cambios muy significativos son los que se ha descrito a lo largo de este documento, es necesario agregar más procedimientos, robustecer o fortalecer los procedimientos y políticas existentes.	Implementar tareas o actividades, procedimientos y políticas que se han descrito anteriormente como: Diagramas de red, sistemas configurados según las normas de configuración, sistemas protegidos con los controles requeridos, que los datos confidenciales no se almacenen, análisis de vulnerabilidades trimestralmente y se incluyan los nuevos sistemas en este.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
6.5	**Aborde las vulnerabilidades de codificación comunes en los procesos de desarrollo de *software* de la siguiente manera: Capacite a los desarrolladores, por lo menos anualmente, en las técnicas actualizadas de codificación segura, incluida la forma de evitar las vulnerabilidades de codificación comunes. Desarrolle aplicaciones basadas en directrices de codificación seguras.**	Inicial	El desarrollador identifica técnicas básicas de seguridad en la codificación segura, pero no está capacitado formalmente en técnicas actualizadas de codificación segura.	Asegurarse que por lo menos anualmente se capacite al personal desarrollador de la compañía en técnicas seguras de codificación, incluida las formas de evitar las vulnerabilidades más comunes. Los desarrollos en la compañía deben basar en estas normas de codificación segura. Estar normas de codificación segura puede ser la guía de la OWASP, estándares de codificación segura CERT, entre otros. Dentro de las políticas se debe incluir la capacitación en codificación segura actualizada que debe tener los desarrolladores.
6.5.1	Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.	Inicial	Aunque a nivel del desarrollo de la aplicación se bloquean consultas basadas en parámetros, bloqueo de caracteres y otros aspectos para bloquear ataques por inyección SQL, estos no son documentados dentro de las buenas prácticas de codificación segura.	Se debe involucrar en el procedimiento documentado de desarrollo técnicas de codificación que aborden los errores de inyección
6.5.2	Desbordamiento de *buffer*	No existe	En las validaciones de seguridad, ni en la codificación se involucra técnicas contra el desbordamiento de *buffer*.	Se debe generar en la codificación y en el procedimiento documentado de desarrollo técnicas de codificación que aborden los desbordamientos de *buffer*, con aspectos como validación de límites de *buffe*r y truncamiento de cadenas de entrada. Esto también se debe validar en las pruebas de seguridad.
6.5.3	Almacenamiento cifrado inseguro	No existe	No existen procedimientos ni actividades en la codificación que establezcan almacenamiento criptográfico seguro.	Se debe generar en la codificación y en el procedimiento documentado de desarrollo técnicas de codificación que aborden el almacenamiento de cifrado seguro, con verificaciones que prevengan el cifrado inseguro y uso de claves y algoritmos de cifrado seguros.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
6.5.4	Comunicaciones inseguras	No existe	No existen procedimientos ni actividades en la codificación que establezcan técnicas de codificación que autentiquen y cifren correctamente todas las comunicaciones confidenciales.	Se debe generar en la codificación y en el procedimiento documentado de desarrollo técnicas de codificación que autentiquen y cifren correctamente todas las comunicaciones confidenciales. Se pueden usar cifrado simétrico a nivel LAN en el uso de aplicaciones con algoritmos como AES256.
6.5.5	Manejo inadecuado de errores	Inicial	No existen procedimientos ni actividades en la codificación que verifique el manejo inadecuado de errores. A nivel práctico si se ejecutan algunas técnicas en el manejo de errores, pero no es un procedimiento formal.	Se debe generar en la codificación y en el procedimiento documentado de desarrollo el manejo adecuado de errores, para evitar exponer información privilegiada mediante métodos de manejo de errores.
6.5.6	Todas las vulnerabilidades de “alto riesgo” detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.1 de las PCI DSS).	Definido	Las vulnerabilidades en criticidad alta y media identificadas son solucionadas y son regidas mediante indicadores en las cuales las vulnerabilidades altas se deben resolver en 15 días y las medias en 45 días.	Los indicadores relacionados con la solución de vulnerabilidades deben estar directamente relacionados con los indicadores que rigen al proceso de desarrollo, las vulnerabilidades en alta detectadas, deben ser solucionados y aplicados en las aplicaciones en producción y corregidos en las que están en el proceso de desarrollo.
6.5.7	Lenguaje de comandos entre distintos sitios (XSS)	Inicial	Cuando se realizan las verificaciones de seguridad antes de que la aplicación salga a producción, se realizan verificaciones relacionadas a ataque XSS (*Cross-site scripting*), estas pruebas no están documentadas en el procedimiento o políticas su debida revisión.	Documentar en el procedimiento o políticas las técnicas de codificación que incluyan validación de todos los parámetros antes de la inclusión y uso de técnicas de escape sensibles al contexto
6.5.8	Control de acceso inapropiado (como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios, y la no restricción de acceso a las funciones por parte de los usuarios).	Inicial	Aunque en el desarrollo de aplicaciones si se tiene en cuenta la referencia directa insegura a objetos, y es probada en las pruebas de seguridad, este procedimiento no está documentado ni está establecido en las políticas de desarrollo.	Se debe generar en la codificación y en el procedimiento documentado de desarrollo el manejo de referencia directa insegura a objetos, que incluya aspectos como autenticación correcta de usuarios, desinfección de entradas, no exposición de referencias a objetos internos a usuarios.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
6.5.9	Falsificación de solicitudes entre distintos sitios (CSRF)	No existe	No existe procedimientos ni actividades en la codificación que verifique la falsificación de solicitudes entre distintos sitios (CSRF)	Se debe generar en la codificación y en el procedimiento documentado de desarrollo actividades para la corrección de CSRF (falsificación de solicitudes entre distintos sitios) y solucionar esta vulnerabilidad en las aplicaciones que ya estén en producción
6.5.10	Autenticación y administración de sesión interrumpidas	No existe	No existe procedimientos ni actividades en la codificación que verifique la autenticación y la administración de sesión interrumpidas.	Se debe generar en la codificación y en el procedimiento documentado de desarrollo actividades como *tokens* de sesión, no exposición de los ID de la sesión en la URL y la incorporación de tiempos de espera apropiados y rotación de las ID de la sesión después de iniciar sesión satisfactoriamente.
6.6	**En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente y asegúrese de que estas aplicaciones se protejan contra ataques conocidos con alguno de los siguientes métodos: Controlar las aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, por lo menos, anualmente y después de cada cambio**	Definido	No existe ninguna aplicación publica que maneje información del titular de la tarjeta o tarjeta, sin embargo las aplicaciones que son de acceso público en la compañía están alojadas en el servidor DMZ. De igual manera el análisis semestral en análisis de vulnerabilidades que se realiza involucre el servidor de DMZ, como también todas las aplicaciones antes de salir a producción en el servidor DMZ, se realizan las respectivas revisiones de seguridad por el oficial de seguridad. Existe un *firewall* que esta entre la red pública y el servidor DMZ. Se han realizado prácticas de hardening en el servidor que aloja las aplicaciones públicas.	Involucrar en el procedimiento de desarrollo, la solución de las vulnerabilidades detectadas, además de realizar validaciones de seguridad cuando las aplicaciones que son accedidas a nivel LAN deben ser accedidas en un momento determinado desde el servidor DMZ. Se debe involucrar un análisis de seguridad de vulnerabilidades de las aplicaciones por lo menos una vez al año. Se sugiere tener *logs* de auditoria que aplique en la política relacionada a la DMZ, implementar en la política del *firewall* parámetros de IPS además de implementar un equipo IDS, con un WAF por ejemplo un ModSecurity.
6.7	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones estén documentados, implementados y que**	Definido	Se encuentra documentadas las políticas de seguridad de la información en el proceso de desarrollo. Aún falta involucrar dentro del proceso de desarrollo la solución de vulnerabilidades. Esta documentación esta publica y es de conocimiento a las partes interesadas.	Involucrar en el procedimiento de desarrollo la solución de todas la vulnerabilidades detectadas en los sistemas y aplicaciones, de igual manera la solución de todas las falencias de seguridad en los cambios realizados o las nuevas aplicaciones que van a salir al ambiente de producción.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	sean de conocimiento para todas las partes afectadas.			
Requisito 7	**Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.**			
7.1	**Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso.**	Inicial	Esta establecida una política de control de acceso a la información, pero debe ser más descriptiva sobre el nivel de información a la cual se tiene acceso. Existen varios perfiles como son los analistas de calidad, analistas de estadística, desarrollador y asesores tiene acceso a información que no es necesaria para poder ejercer su labor correctamente y corresponde a información de los titulares de la tarjeta y datos de la tarjeta	Se debe definir, establecer y documentar parámetros más restrictivo a la información que accede los funcionarios de la compañía dependiendo de cada cargo o función. Limitar el acceso a los datos de los titulares de la tarjeta.
7.1.1	Defina las necesidades de acceso de cada función, incluso lo siguiente: Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. Nivel de privilegio necesario (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.	Inicial	Existen roles, cargos, funciones, políticas de control de acceso a la información, procedimiento de gestión de usuarios y uno de roles y privilegios, pero no está definidos los componentes del sistema y el nivel de privilegio que de tener cada cargo para poder ejercer su labor.	Se debe definir por cargo o perfil los componentes del sistema a los cuales debe tener acceso con el fin de que ejerza su labor y el nivel de privilegio.
7.1.2	Limite el acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo.	Inicial	Existen roles, cargos, funciones, políticas de control de acceso a la información, procedimiento de gestión de usuarios y un procedimiento de roles y privilegios, pero no está definidos el nivel de privilegio que de tener cada cargo para poder ejercer su labor.	Establecer los cargos o funciones específicas que deben tener acceso a la información privilegiada con el fin que este limitada. Estos accesos privilegiados deben cumplir parámetros como que la asignación solo se asigne a funciones que específicamente necesitan acceso privilegiado y estén asignados a la menos cantidad posible.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
7.1.3	Asigne el acceso según la tarea, la clasificación y la función del personal.	Inicial	Existen roles, cargos, funciones, políticas de control de acceso a la información, procedimiento de gestión de usuarios y un procedimiento de roles y privilegios, no está definido que los privilegios se asignen según la clasificación de la información y la función laboral de la persona.	Definir y documentar el asignamiento de privilegios a los funcionarios o cargos de acuerdo a la clasificación de la información, función laboral de la persona que ya está creado en Intercontact.
7.1.4	Solicite la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios.	Inicial	Existe un procedimiento de creación de usuarios, asignación de roles y privilegios pero este no esta tan completo para determinar el nivel de acceso a la información que debe acceder el perfil o el funcionario.	Complementar el procedimiento de asignación de roles y privilegios, para determinar el debido procedimiento para asignar el nivel de acceso o privilegios que va a tener el funcionario, de igual manera vincular en el perfil del funcionario los privilegios a los cuales este puede acceder de acuerdo al cargo. No se pueden asignar privilegios sin pasar por un debido procedimiento de aprobación.
7.2	**Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo", salvo que se permita específicamente.**	Inicial	Existe un procedimiento de creación, modificación y eliminación de usuarios, se asignar permisos a componentes del sistema, carpetas, acceso a redes externas como internet, de acuerdo a un perfil por ejemplo, asesor, supervisor, admirativo. No está muy bien definido cada uno de los cargos o roles, ni la información que puede o podría tener acceso.	Se debe reforzar el procedimiento de creación, modificación y eliminación de usuarios en los que se relacione el cargo con el debido perfil para poder limitar con mayor cuidado el acceso a componentes del sistema, información, privilegios, accesos, entre otros.
7.2.1	Cobertura de todos los componentes del sistema	Inicial	Todos los componentes del sistema tienen un debido control de acceso pero no están formalmente definidos de que perfiles o cargos deben tener acceso o privilegios sobre el sistema.	Documentar que el control de acceso se implemente en todos los componentes del sistema.
7.2.2	La asignación de privilegios a una persona se basa en la clasificación del trabajo y su función.	Inicial	Existe un procedimiento de creación, modificación y eliminación de usuarios, se asignar permisos a componentes del sistema, carpetas, acceso a redes externas como internet, de acuerdo a un perfil por ejemplo, asesor, supervisor, admirativo. No está muy bien definido cada uno de los cargos o roles, ni la información que puede o podría tener acceso.	Se deben definir de manera más precisa los perfiles de cada funcionario relacionado al acceso de información a la cual debe tener acceso, esto con el fin de determinar el nivel de acceso relacionado a los componentes del sistema e información debe tener. Esto con el fin de fortalecer el procedimiento de creación, modificación y eliminación de usuarios.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
7.2.3	Configuración predeterminada de "negar todos".	Definido	A nivel de *firewall* (acceso a internet, redes externas), controlador de dominio (acceso a la estación de trabajo, carpetas compartidas) y aplicaciones esta definidas para que el acceso este en denegado solo hasta se haya creado el respectivo usuario.	Se deben definir de manera más precisa los perfiles de cada funcionario relacionado al acceso de información a la cual debe tener acceso, esto con el fin de determinar el nivel de acceso relacionado a los componentes del sistema e información debe tener. Esto con el fin de fortalecer el procedimiento de creación, modificación y eliminación de usuarios.
7.3	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.**	No existe	No existe documentación que defina la restricción de acceso a los datos del titular de la tarjeta.	Dentro de las políticas de seguridad y procedimientos se debe definir la restricción el acceso a los datos del titular y que esto sea de conocimiento de las partes interesadas y se aplique.
Requisito 8:	**Identificar y autenticar el acceso a los componentes del sistema.**			
8.1	**Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema**	Definido	Existe un controlador de dominio que otorga el usuario y las claves de acceso a las estaciones de trabajo, también un aplicativo de gestión que otorga usuario y contraseña a todas las aplicaciones de la compañía. Estos otorgan permisos o privilegios de acuerdo a un rol definido con anterioridad.	Se debe generar un seguimiento más juicioso a los *logs* de logueo de usuarios para evidenciar ciertos eventos o incidencias. Establecer las debidas restricciones de acceso a los datos del titular descritas con anterioridad.
8.1.1	Asigne a todos los usuarios una ID exclusiva antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.	Inicial	Todos los funcionarios de la compañía tienen un ID único acompañado de una contraseña para acceder a las estaciones de trabajo y a las aplicaciones, dado que el aplicativo FTP que es otorgado por el cliente este otorga un solo ID y contraseña que es usado por dos funcionarios de la compañía, las grabaciones y audios de llamadas que contiene datos del titular también son accedidas con ID y contraseñas únicas	Solicitar al cliente Metlife la creación de perfiles con respectivo ID y usuario para identificar y determinar cada rol y usuario y a qué nivel de privilegios puede acceder, lo mismo controlar el nivel de acceso con relación a las llamadas y grabaciones que contiene datos del titular de la tarjeta como anteriormente se había nombrado.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
8.1.2	Controle la incorporación, la eliminación y la modificación de las ID de usuario, las credenciales y otros objetos de identificación.	Definido	Existe un procedimiento de creación, modificación y eliminación de usuarios que otorga un ID único y cambio de al primer acceso, el cambio de contraseña es obligatorio y es cada 30 días, el proceso de modificación o eliminación se realiza cada vez que un funcionario es desvinculado de la compañía o es cambiado de cargo.	En varias ocasiones en el cambio de cargo no se realiza la solicitud de modificación de perfiles o acceso a todas la plataformas, estas pueden incluir el acceso a la los datos del titular de tarjeta, formalizar de manera adecuada este procedimiento. Esto debe involucrar el nivel de acceso o privilegios que debe tener a los sistemas o a la información
8.1.3	Cancele de inmediato el acceso a cualquier usuario cesante.	Inicial	Existe un procedimiento de creación, medicación y eliminación de usuarios en Intercontact, cuando un funcionario desvinculado de la compañía sus usuarios no son cancelados o inactivados pero esto no se realiza de manera inmediata, existe un procedimiento de paz y salvo pero tampoco es muy efectivo, la solicitud de eliminación de usuarios puede pasar un tiempo no prudente para enviar la debida solicitud.	Se debe realizar la eliminación o deshabilitación de usuarios de todas las plataformas y sistemas incluido los sistemas de acceso físico lo más rápido posible. El procedimiento de paz y salvo debe ser más efectivo con el fin que el funcionario este a paz a salvo antes de abandonar la compañía.
8.1.4	Elimine o inhabilite las cuentas de usuario inactivas, al menos, cada 90 días.	Inicial	Existe un script que se desarrolló con el fin de eliminar todas las cuentas desactivadas de usuario del directorio activo cada cierto periodo de tiempo, falta definir que sea máximo 90 días que en las otras plataformas se aplique de igual manera.	Definir documentalmente que las cuentas de usuario desactivadas en el directorio activo se eliminen máximo cada 90 días, también establecer que todas las cuentas de usuario de las demás plataformas también sean eliminadas máximo cada 90 días.
8.1.5	Administre las ID que usan los terceros para acceder, respaldar o mantener los componentes del sistema de manera remota de la siguiente manera: *Se deben habilitar solamente durante el tiempo que se necesitan e inhabilitar cuando no se usan. * Se deben monitorear mientras se usan.	Inicial	Los proveedores o terceros que acceden a los sistemas para prestar algún servicio a Intercontact solo pueden acceder mediante un acceso VPN que es previamente configurado con usuario y contraseña único, no se realiza ningún tipo de monitoreo mientras estos usan el servicio. Algunas plataformas son de propiedad de los proveedores y el acceso a esta no está debidamente definido o limitado.	Se debe realizar el debido monitoreo de los proveedores o terceros mientras acceden a los sistemas. Se deben deshabilitar mientras estas no se usen. Establecer horarios de acceso con el fin que solo se usen cuando el proveedor las use y se deshabiliten cuando ya no esté en uso. Se debe establecer los criterios de acceso a los proveedores y terceros para que estos no accedan a ciertos privilegios o tengan acceso a información que no debería ser de su conocimiento.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
8.1.6	Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.	Definido	El acceso a las estaciones de trabajo y a las aplicaciones desarrolladas *In-house* incluyendo la aplicación que maneja los datos del titular de la tarjeta y la tarjeta se bloquean después de 5 intentos erróneos de ingreso a la aplicación. No está involucrado la plataforma de telefonía en esta configuración	Actualizar las políticas o procedimientos estableciendo que el máximo ingreso de ID y contraseña erróneo a los diferentes sistemas no debe superar 6 intentos. Se debe involucrar y todos los sistemas en los cuales el usuario final tiene acceso. Se debe involucrar la plataforma de telefonía en esta configuración. Solicitar al cliente Metlife que el aplicativo FTP se bloquee el usuario cuando se ingrese la contraseña erróneamente 6 veces incorrectamente
8.1.7	Establezca la duración del bloqueo a un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.	Inicial	El bloqueo de inicio de sesión en las estaciones de trabajo solo está establecido en 5 minutos, mientras el bloqueo de usuarios en la aplicaciones usadas por los funcionarios si se debe realizar una solicitud pro la plataforma de *help desk* para solicitar su debido desbloqueo por el administrador.	Se debe establecer en los procedimientos o en las políticas de la compañía que el bloqueo de las cuentas de usuario cuando se bloqueen permanezcan mínimo 30 minutos bloqueadas o que su desbloqueo se realice directamente por el administrador del sistema. Se debe ampliar el bloqueo de sesión por errores continuos en el ingreso de contraseña mino a 30 minutos. Se debe involucrar la plataforma de telefonía en esta configuración. Solicitar al cliente Metlife que cuando se bloquee el usuario mínimo dure 30 minutos bloqueado o que el desbloqueo sea realizado directamente por el administrador de la plataforma
8.1.8	Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para activar la terminal o la sesión nuevamente.	Definido	En el directorio activo está configurado para que las sesiones de las estaciones de trabajo se bloqueen cada 3 minutos si la sesión mantiene inactiva, en las aplicaciones si está configurada de diferentes maneras depende de la aplicación, unas están en 15 minutos otras en 1 hora.	Actualizar las políticas de escritorio limpio y pantalla limpia indicando que el máximo tiempo que una sesión este inactiva antes de que vuelva a solicitar de nuevo ingreso de usuario y contraseña es 15 minutos, esto debe aplicar para todos los sistemas (directorio activo, planta telefónica, aplicaciones, entre otros). Solicitar al cliente Metlife esta configuración de sesión inactiva en el servicio FTP y VPN que se tiene configurada.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
8.2	**Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar todos los usuarios: Algo que el usuario sepa, como una contraseña o frase de seguridad. Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente. Algo que el usuario sea, como un rasgo biométrico.**	Repetible	En el inicio de sesión en las estaciones de trabajo aparte de tener una ID de usuario para ingresar al sistema requiere de una contraseña, lo mismo sucede en las aplicaciones de la compañía. En el acceso físico a las instalaciones o dependencias se utiliza un sistema de doble autenticación que es el uso de una tarjeta de acceso y de un sistema biométrico.	Documentar los métodos de autenticación que se usa en Intercontact en los diferentes sistemas incluyendo los accesos físicos y las aplicaciones otorgadas por el cliente Metlife.
8.2.1	Deje ilegibles todas las credenciales de autenticación (como contraseñas/frases) durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una criptografía sólida.	Inicial	En las aplicaciones usadas a nivel interno en la compañía y que se usa para el ingreso de datos del titular de la tarjeta utiliza un método para que estas no viajen en texto plano no se determina que estos utilicen criptografía sólida, lo mismo las claves ingresadas en el inicio de sesión en las estaciones de trabajo y en la aplicación FTP.	Actualizar las políticas estableciendo que las contraseñas deben estar ilegibles durante su trasmisión y almacenamiento en los sistemas utilizados por Intercontact. Esta información debe ser ilegible mediante el uso de una criptografía sólida como AES256 o con el uso de un hash como SHA1 o superior. Se debe involucrar en esto los sistema como el directorio activo, los *Acces point,* las aplicaciones, bases de datos, servidor planta telefónica, entre otros.
8.2.2	Verifique la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablezca la contraseña, entregue nuevos *tokens* o genere nuevas claves.	Inicial	En el procedimiento de restablecimiento de contraseña o desbloqueo de usuario se realiza mediante una solicitud en el aplicativo de *service desk* por el jefe directo del funcionario que tiene esta cuenta bloqueada, sin embargo este criterios no se aplica para todos los cargos. No existe uno pasos o procedimiento documentando estableciendo los criterios que se deben ejecutar para efectuar un desbloqueo o	Actualizar el procedimiento o políticas de Intercontact indicando el debido procedimiento de desbloqueo o restablecimiento de contraseña con el fin de garantizar que realmente la persona que solicita el desbloqueo o restablecimiento de la contraseña sea la correcta o al propietario de la misma.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
			restablecimiento de una contraseña o una cuenta de usuario.	
8.2.3	Las contraseñas/frases deben tener lo siguiente: Una longitud mínima de siete caracteres. Combinación de caracteres numéricos y alfabéticos. De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.	Definido	Existe un procedimiento de gestión de usuarios y contraseñas que establece los procedimientos que rigen el uso de contraseña que encierra parámetros como son longitud mínima de 8 caracteres, uso de mayúsculas y minúsculas, números y caracteres especiales.	El procedimiento de gestión de usuarios y contraseñas debe regir en todos los sistemas que involucran los datos del titular de la tarjeta como son el aplicativo de la planta telefónica (acceso a grabaciones), FTP proporcionado por el cliente y todas las aplicaciones.
8.2.4	Cambie la contraseña/frase de usuario, al menos, cada 90 días.	Repetible	Los sistemas como el directorio activo y la mayoría de aplicaciones tiene por política el cambio de contraseña obligatorio cada 30 días, estas contraseñas deben cumplir obligatoriamente con ciertos parámetros nombrados con anterioridad como son de longitud mínima de 8 caracteres, uso de mayúsculas, minúsculas, números y caracteres especiales.	Actualizar políticas o el procedimiento de gestión de contraseñas y usuarios con el fin de establecer que los sistemas soliciten al usuario la renovación de su contraseña mínimo cada 90 días, se deben involucrar todos los sistemas que están relacionados con los datos del titular de la tarjeta como son los aplicativos de la planta telefónica (mitrol) y los aplicativos proporcionados por el cliente Metlife (VPN, FTP)
8.2.5	No permita que una persona envíe una contraseña/frase nueva que sea igual a cualquiera de las últimas cuatro contraseñas/frases utilizadas.	Repetible	El directorio activo tiene histórico de las ultimas 20 contraseñas con eso el usuario no puede repetir las ultimas 20 contraseña, está en producción que esto se aplique a nivel de todos los aplicativos. Esto no está configurado en el aplicativo Mitrol (telefonía) ni en los aplicativos otorgados por el cliente Metlife	Actualizar el procedimiento de gestión de usuario y contraseñas o en las políticas que todos los sistemas que involucren los datos del titular de la tarjeta el bloqueo de uso repetido de contraseña por lo menos las últimas cuatro contraseñas, solicitar que esto también se realice en los aplicativos proporcionados por el cliente Metlife
8.2.6	Configure la primera contraseña/frase y las restablecidas en un valor único para cada usuario y cámbiela de inmediato después del primer uso.	Repetible	Los sistemas como el directorio activo y la mayoría de aplicaciones tiene por política el cambio de contraseña en el primer ingreso dado que cuando se asigna el usuario por primera vez la contraseña otorgada al funcionario o tercero es una genérica o su número de cedula.	Actualizar el procedimiento de gestión de usuarios o contraseñas o las políticas de Intercontact estableciendo el cambio de contraseña en el primer ingreso al sistema en el caso de las estaciones de trabajo, aplicaciones, Mitrol, entre otros.
8.3	**Asegure todo el acceso administrativo**	No existe	No existe autenticación de doble factor, el único método de autenticación de doble factor que	Se debe implementar un sistema de autenticación de doble factor a nivel de acceso

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	individual que no sea de consola y todo el acceso remoto al CDE mediante la autenticación de múltiples factores.		existe es el acceso físico a las instalaciones.	administrativo individual que no sea de consola y todo acceso remoto al entorno de los datos del titular de la tarjeta. La autenticación de múltiples factores puede realizarse, ya sea tras la autenticación para la red en particular o para el componente del sistema. Por ejemplo en el acceso a la base de datos donde esta los datos del titular de la tarjeta
8.3.1	Incorporar la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE para el personal con acceso administrativo.	No existe	Solo se maneja autenticación de doble factor para el ingreso físico a las instalaciones u diferentes áreas de INTERCONTACT. Si existe segmentación de red para separar la red del CDE del resto de redes, pero los servidores de directorio activo, telefonía (grabaciones), aplicaciones y bases de datos es utilizado con otras redes	Involucrar autenticación de múltiple factor en los entornos que no se accede mediante consola como es el acceso a la bases de datos y a la grabaciones que contiene datos del titular de la tarjeta. Esta autenticación de doble factor se puede emplear por ejemplo el envió de un correo electrónico con un clave a parte de la clave ya usada para ingresar al sistema.
8.3.2	Incorpore la autenticación de múltiples factores para todo acceso remoto que se origine desde fuera de la red de la entidad (tanto para usuarios como administradores, e incluso para todos los terceros involucrados en el soporte o mantenimiento).	No existe	Solo se maneja autenticación de doble factor para el ingreso físico a las instalaciones u diferentes áreas de INTERCONTACT. El acceso remoto desde fuera de la red de Intercontact, se realiza únicamente por VPN site to client con usuario y contraseña definidos.	Involucrar autenticación al menos de doble factor en el acceso remoto por los administradores del sistema y proveedores que podrían tener acceso a los datos del titular de la tarjeta por ejemplo el proveedor de telefonía Mitrol, se puede implementar tokens, o la recepción de un SMS o correo electrónico con un código para poder ingresar, a parte del uso de la contraseña.
8.4	**Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios, que incluye lo siguiente: Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. Instrucciones para no seleccionar contraseñas utilizadas**	Definido	Intercontact cuenta con el procedimiento para la gestión de usuarios, contraseñas, perfiles y privilegios, en este procedimiento se indica la manera adecuada de asignar usuarios, creación de contraseñas seguras como es el uso de mínimo 8 caracteres con el uso de minúsculas, mayúsculas, números y caracteres especiales. Además se cuenta con una Política de claves. Esta política y procedimiento es de conocimiento y está al alcance de todos los funcionarios de la compañía.	Completar el procedimiento de gestión de usuarios, contraseñas, perfiles indicando las buenas prácticas para proteger las credenciales de autenticación no escribir las contraseñas ni guardarlas en archivos no seguros y estar atentos a personas malintencionadas que intenten hurtar sus contraseñas (por ejemplo, llamar a un empleado y solicitar su contraseña para poder "solucionar el problema"), el prohibido uso de contraseñas usadas con anterioridad, configuración de esto en los diferentes sistemas para que no permita usar por lo menos las últimas 4 contraseñas usadas.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	anteriormente. Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos.			Los pasos a seguro para cambiar las contraseñas en los sistemas si se sospecha que esta contraseña está corriendo riesgos. También completar en el procedimiento una pequeño instructivo de cómo elegir una contraseña segura, por ejemplo el uso de palabras de diccionario, datos de la persona como nombres de familiares, fechas, entre otros.
8.5	**No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación de la siguiente manera: Las ID de usuario genéricas se deben desactivar o eliminar. No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas. Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema.**	Repetible	Por políticas de seguridad está prohibido el uso de contraseñas o ID genéricos, solo las salas de capacitación utilizan un usuario genérico, las redes de estas salas están debidamente segmentadas y aisladas de las otras redes, de igual manera este usuario solo se puede usar en estas salas de capacitación, está bloqueado este usuario si se quiere utilizar en cualquier estación de trabajo. Se utiliza una cuenta administrativa para la configuración de equipos cuando todavía no están en el dominio	Se debe deshabilitar el usuario administrativo utilizado para realizar configuraciones en las estaciones de trabajo o servidores, cada funcionario de soporte debe utilizar un usuario individual con ciertos niveles o privilegios para realizar las debidas configuraciones que son requeridas para ejecutar sus labores.
8.5.1	Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios que tengan acceso a las instalaciones del cliente (por ejemplo, para tareas de soporte de los sistemas de POS o de los servidores) deben usar una credencial de autenticación exclusiva (como una contraseña/frase) para cada cliente.	No Aplicable	La compañía INTERCONTACT no realiza actividades en las cuales se involucre el acceso a las instalaciones de los clientes. No se realizan transacciones en la campaña Metlife, solo se realiza la recolección de datos.	La compañía INTERCONTACT no realiza actividades en las cuales se involucre el acceso a las instalaciones de los clientes.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
8.6	**Si se utilizan otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.), el uso de estos mecanismos se debe asignar de la siguiente manera: Los mecanismos de autenticación se deben asignar a una sola cuenta y no compartirlos entre varias. Se deben implementar controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.**	Inicial	Solo se utiliza autenticación de doble factor en el acceso físico a las instalaciones o diferentes áreas, con el uso de una tarjeta y la huella digital, este sistema de autenticación es asignado a cada persona dado que si se utiliza una tarjeta que no corresponda a la huella enrolada esta no sirve. No se utiliza otros sistemas de autenticación en la compañía que involucre el uso de tokens, certificados, etc.)	Identificar que otros sistemas deben reforzar el sistema de autenticación, e involucrar sistemas de autenticación dobles o triples, por ejemplo servidores de bases de datos o donde se alojan las grabaciones.
8.7	**Se restringen todos los accesos a cualquier base de datos que contenga datos del titular de la tarjeta (que incluye acceso por parte de aplicaciones, administradores y todos los otros usuarios)**	Inicial	Solo un funcionario puede tener acceso a la base de datos que contiene los datos del titular de la tarjeta, con permisos de lectura, escritura. Este funcionario asigna los permisos de consulta a la base a otros funcionarios que necesitan consultar las bases para ejercer sus funciones. No existen métodos programáticos para el proceso de acceso, consultas o acciones. Los analistas de estadística pueden acceder directamente a las bases a realizar consultas aunque solo sea de consulta. Solo las aplicaciones usan ID de aplicaciones para las apelaciones de bases de datos. Todos los usuarios son autenticados antes del ingreso a cualquier aplicación o a la base de datos si es el caso. Los acceso a la base de datos está limitado al administrado de Base de datos	Se deben realizar configuraciones para que solo el administrador de la base de datos sea el único que puede acceder directamente a la base de datos para realizar consultas. Los métodos de acceso, consulta, mover, copiar y eliminar en la base de datos se deben realizar únicamente mediante métodos programáticos, por ejemplo a través de procedimientos almacenados y no, a través del acceso directo a la base de datos por parte de usuarios finales

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
8.8	**Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados, implementados y que sean de conocimiento para todas las partes afectadas**	Definido	Existen política de seguridad sobre el uso de claves, procedimientos de gestión de usuarios y claves, existe el procedimiento de creación, modificación y eliminación de usuarios. Configuración a nivel de sistemas y aplicaciones en los cuales se bloqueó el usuario luego de ingresar la contraseña errada un número determinado de veces. El cambio obligatorio de contraseña es obligado a nivel de estación de trabajo y de aplicaciones	Actualizar documentación del procedimiento y políticas con lo establecido con anterioridad, por ejemplo el uso repetitivo de contraseñas, cambio periódico de contraseña, bloqueo de usuarios por número errado de intentos, entre otros.
Requisito 9	**Restringir el acceso físico a los datos del titular de la tarjeta.**			
9.1	**Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.**	Inicial	El acceso a la entrada principal requiere la lectura de una tarjeta para habilitar un torniquete, el acceso a los diferentes pisos requiere el uso de la misma tarjeta pero acompañado con el uso de la huella. El área donde están ubicado los asesores y supervisores de Metlife no está totalmente separados de otras campañas. Los analistas de calidad que tiene acceso a las grabaciones que tiene datos del titular comparten lugar con otros analistas y están ubicados en otras campañas. El analista de estadística también está ubicado en un área donde comparte con otros analistas que no tiene relación con la campaña Metlife. La deficiencia de tarjetas biométricas por la rotación constante de personal, hace que muchas de las puestas mantengan abiertas. El *datacenter* tiene seguridad dado que su entrada es mediante uso de biométrico y solo tiene acceso los del área de tecnología. Por políticas de directorio activo se bloquea cada 3 minutos las sesión cuando no hay actividad, de igual manera en las aplicaciones las sesiones se terminan después de 10 minutos	Adquirir un *stock* suficiente de tarjetas, al igual que mejorar el proceso de descuentos de las tarjetas adquiridas con el fin de comprar las tarjetas extraviadas lo más pronto posible. Controlar el acceso al área donde está ubicada la campaña Metlife y trasladar a los funcionarios analistas de calidad y alcista de estadística donde está ubicada la campaña Metlife.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
9.1.1	Utilice cámaras de video u otros mecanismos de control de acceso (o ambos) para supervisar el acceso físico de personas a áreas confidenciales. Revise los datos recopilados y correlaciónelos con otras entradas. Guárdelos durante al menos tres meses, a menos que la ley estipule lo contrario.	Repetible	Existen cámaras en todos los pisos y mayorías de áreas de la compañía tanto en espacios públicos como oficinas, en cada piso existe un DVR de cámaras que es administrado por algún funcionario de tecnología, el acceso a esta grabaciones necesita un ID y una contraseña que solo es de conocimiento del funcionario delegado para tal fin, estas están grabando 7 *24. Existe grabaciones disponibles de por lo menos los ultimo 6 meses	No existe un diagrama de distribución de cámaras con el fin de ubicar las cámaras de manera efectiva para monitorear y controlar los accesos a áreas sensibles de la compañía. Instalar cámaras faltantes en áreas donde se manejan datos del titular, por ejemplo en el área donde están ubicados los analistas de calidad.
9.1.2	Implemente controles físicos o lógicos para restringir el acceso a conexiones de red de acceso público.	Repetible	El acceso inalámbrico a la red de la compañía solo se puede realizar de dos manera, la primera es incluyendo la dirección MAC y la debida contraseña para acceder a la red LAN, este permiso solo se habilita cuando la persona es funcionario de la compañía. Cuando un tercero o visitante necesita acceso, se conecta este mediante una red de visitantes que está aislada de la red LAN y su contraseña es renovada cada semana. Todos los visitantes deben estar acompañados todo momento mientras su permanencia en las instalaciones de Intercontact	Se debe deshabilitar los puntos de red de las salas de juntas, también se debe deshabilitar los puntos de red que no tiene ningún equipo conectado así como también incluir un bloqueo de puertos, por ejemplo que los puertos se bloqueen cuando la dirección Mac relacionada al puerto ha cambiado más de una vez. Actualizar las políticas de seguridad de control de acceso involucrando este tipo de restricciones.
9.1.3	Limite el acceso físico a los puntos de acceso inalámbricos, *gateways,* dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.	Definido	Algunos *Acces point* no están ubicados en sitios que sean de difícil acceso, los demás dispositivos de redes y de comunicaciones si están debidamente ubicados en el datacenter o en los centros de cableado de cada piso, cuyo acceso es debidamente controlado con un sistema biométrico.	Verificar que todo el acceso físico a los dispositivos inalámbricos esté debidamente controlados, dado que algunos *Acces point* no están ubicado en sitios que sean de difícil acceso, ubicar correctamente los *Acces point* que se identifique algún tipo de riesgo.
9.2	**Desarrolle procedimientos que permitan distinguir, fácilmente, a los empleados y a los visitantes, de la siguiente manera: Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). Cambios en los requisitos de acceso.**	Definido	Todos los funcionarios de la compañía cuanta con un carnet que tiene foto y cargo, además de una tarjeta de proximidad que se usa en conjunto con su huella dactilar para ingresar a ciertas áreas de Intercontact que esté debidamente autorizado. La identificación de visitantes o terceros se realiza mediante el uso de carnet, dependiendo de la razón de ingreso, por ejemplo se usa un carnet diferente para los proveedores, personal en formación, en pruebas de selección o visitantes. Para	Deshabilitar las tarjetas de acceso en el menor tiempo posible de los funcionarios que ya no laboren en la compañía, se debe agilizar el procedimiento de paz y salvo para informar de manera inmediata cuando una persona ya no labora en la compañía. Se debe adquirir un *stock* de tarjetas para que los funcionarios de la compañía las tengan y las puertas permanezcan cerradas.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación).		otorgar un carne a un tercero se debe registrar con anterioridad y debe ser debidamente autorizado Los visitantes son acompañados todo el tiempo. El acceso y control de visitantes está establecido por políticas de seguridad de Intercontact. Los lapsos de tiempo de desactivación de las tarjetas de proximidad son demasiado largos.	
9.3	**Controle el acceso físico de los empleados a las áreas confidenciales de la siguiente manera: El acceso se debe autorizar y basar en el trabajo de cada persona. El acceso se debe cancelar inmediatamente después de finalizar el trabajo, y todos los mecanismos de acceso físico, como claves, tarjetas de acceso, se deben devolver o desactivar**	Inicial	Por políticas está establecido procedimiento para el ingreso y estancia dentro de la compañía. El déficit de tarjetas hace que los controles de acceso sean inútiles dado que un funcionario puede ingresar a cualquier área de Intercostal. Los accesos otorgados con las tarjetas de proximidad no son revocados inmediatamente cuando la persona deja de ser funcionario de Intercontact. Muchas de las puertas están dañadas causando que el sistema de control de acceso sea inútil. El acceso a áreas confidenciales como data center o centros de cableados de cada piso están debidamente controlados.	Actualizar las políticas de seguridad estableciendo el control de acceso autorizado relacionado a los permisos otorgados en el momento de entrega de carnet. Se debe adquirir de manera pronta un *stock* de tarjetas y asignarlas por lo menos al personal que están en el área de metlife, con el fin de que solo ingrese el personal autorizado. Se debe aislar la operación de Metlife preferiblemente usando también un control biométrico para garantizar que solo ingresen personal relacionado a esta área. Se deben arreglar puertas que en el momento se encuentran dañadas y no es posible utilizar de manera efectiva el control de acceso y no se tiene control de que personal ingresa a ciertas áreas.
9.4	**Implemente procedimientos para identificar y autorizar a los visitantes.**	Definido	Por políticas de control de acceso están definidos los protocolos que deben cumplir tanto la recepción como el personal de seguridad para el ingreso de personal a las instalaciones de la compañía. El control de visitantes está debidamente establecido.	Controlar de manera más adecuada cuando existe un número considerable de personal en la recepción para evitar el ingreso no controlado de personal por un descuido en la recepción o a nivel de vigilancia. Estos procedimientos deben ser debidamente documentados para estos casos.
9.4.1	Los visitantes reciben autorización antes de ingresar en las áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y estarán acompañados en todo momento.	Definido	Están definidas políticas de control de acceso en las cuales se establecen los lineamientos que debe cumple la recepción como el personal de vigilancia para el acceso a las instalaciones de personal visitante. Este es acompañado en todo momento y son debidamente autorizados antes de su ingreso y debidamente	Controlar de manera más adecuada cuando existe un número considerable de personal en la recepción para evitar el ingreso no controlado de personal por un descuido en la recepción o a nivel de vigilancia, esto ocurre cuando va ingresar personal en formación o cuando hay convocatorias masivas para

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
			identificados por el uso de carnet de visitantes que deber ser siempre visible.	presentar proceso de prueba de ingreso. Estos procedimientos deben ser debidamente documentados para estos casos.
9.4.2	Se identifican los visitantes y se les entrega una placa u otro elemento de identificación con fecha de vencimiento y que permite diferenciar claramente entre empleados y visitantes.	Repetible	Están debidamente establecidos los carnets que son asignados para personal visitante o externo, está debidamente categorizado por ejemplo se asigna uno para proveedores, otro para formación y otro para visitantes. Estos carnets son diferentes del que usa los funcionarios de la compañía. Estos carnets no tiene establecido un método que identifique caducidad o vencimiento	A nivel documental se debe completar las políticas indicando que en el momento de registro del personal visitante este siempre debe presentar un documento con foto y con número de identificación, para poderle otorgar un carnet de visitante. Involucrar un método que pueda demostrar la caducidad de este carnet, muchas compañías optan por el uso de un *sticker* impreso con foto, número de identificación y caducidad.
9.4.3	Los visitantes deben entregar la placa o la identificación antes de salir de las instalaciones o al momento del vencimiento.	Definido	Dado que para la entrega del carnet de visitante se debe dar un documento con foto y número de identificación, para poder ser reclamado a la salida debe devolver el carnet de visitante asignado con anterioridad.	Fortalecer el procedimiento de devolución de carnet de visitante, porque en el momento de que la persona se lleve este documento podría volver a ingresar por que su reporte no está muy bien definido, establecer métodos de vencimiento de carnet para que quede inutilizado este método de acceso.
9.4.4	Se usa un registro de visitantes para llevar una pista de auditoría física de la actividad de los visitantes en las instalaciones, en las salas de informática y en los centros de datos donde se almacenan o se transmiten los datos del titular de la tarjeta. Documente el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico en el registro. Conserve este registro durante tres meses como mínimo, a menos que la ley estipule lo contrario.	Repetible	En Intercontact se usa un libro de control de registro de visitantes o personal externo, además un registro que se realiza en el equipo de recepción donde se ingresan otros datos de manera más especifica que están en el documento con foto y número de identificación que es solicitado para el debido ingreso. El personal visitante es acompañado de manera permanente durante el tiempo de su estancia. Dentro del *data center* o los centros de cableado también se tiene una bitácora de ingreso y salida cuando ingresa una persona externa que no pertenece a tecnología	Documentar en las políticas el uso del libro de registro en la recepción, indicando cuales son los campos que debe diligenciar. Completar el registro de acceso indicando la persona o funcionario que autoriza su ingreso y quien realizara el acompañamiento permanente del mismo, también de la empresa que viene y los motivos por los cuales desea ingresar a Intercontact. Este registro debe permanecer por lo menos tres meses disponibles para su debida consulta.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
9.5	**Proteja físicamente todos los medios**	Definido	Para acceder a los datos del titular existen varios controles que están definidos entre políticas procedimientos, por ejemplo los controles ejercidos por el directorio activo (ID, contraseña de inicio de sesión, bloqueo de estación cada 3 minutos, uso de dispositivos removibles, entre otros) las aplicaciones también ejercen autenticación, a nivel de documentación física existe políticas de escritorio limpio y pantalla limpia que prohíbe el uso de documentación física encima de los escritorito sin el debido custodio.	Dar cumplimiento cabal de las políticas, para evitar debidas violaciones e incidentes por robo o manipulación de la información.
9.5.1	Almacene los medios de copias de seguridad en un lugar seguro, preferentemente, en un lugar externo a la empresa, como un centro alternativo o para copias de seguridad, o en un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo.	Repetible	Existen políticas de *backup* de los diferentes sistemas, equipos o información, está establecido la ejecución de pruebas de *Backups* cada dos meses, esto se realiza en un servidor NAS	Realizar el debido *backup* de la NAS de la sede de Calle 63 a la sede de Zona franca de los datos del titular de la tarjeta alojados en las bases de datos y grabaciones para garantizar el almacenamiento del *backup* en un lugar que no sea a nivel local. Se deben aplicar prácticas de *hardening* en los servidores NAS con el fin de realizar el almacenamiento en un sitio seguro, también se recomienda realizar auditorías a este mismo servidor con el fin de garantizar la efectividad de los controles.
9.6	**Lleve un control estricto de la distribución interna o externa de todos los tipos de medios**	Repetible	Existe un procedimiento de transferencia de información que especifica la información que es transportada por medio externos debe ser debidamente cifrada. La única información que contiene información de datos del titular de la tarjeta en un medio externa es un CD de grabaciones que solicita el cliente Metlife sea enviado cada mes, para este caso se comprime el archivo de grabaciones y se cifra en AES256, la clave de descifrado se envía directamente al cliente que la va a descifrar la persona o empresa encargada de transportar de un lado a otro el CD no tiene conocimiento de la clave.	Actualizar inventario de activos, inventariando y clasificando las grabaciones que contiene datos del titular de la tarjeta como confidencial.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
9.6.1	Clasifique los medios para poder determinar la confidencialidad de los datos.	No existe	Tanto las grabaciones alojadas en el servidor de telefonía como el CD que es transportado al cliente no están debidamente registrados en el inventario de activo y tampoco está su debida clasificación.	Actualizar inventario de activos, inventariando y clasificando las grabaciones que contiene datos del titular de la tarjeta como confidencial así mismo el CD utilizado para guardar y enviar esta información al cliente
9.6.2	Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.	No existe	Existe un procedimiento establecido de clasificación de la información la cual determina que la información clasificada como confidencial se debe cifra, dado que no está clasificada la información como bases de datos, tablas o informes que tengan datos del titular y grabaciones que contiene datos del titular de la tarjeta como información confidencial, si esta en algún momento se envía por correo u otro medio no se envía cifrada. No siempre se utiliza una empresa de envió para enviar el CD con grabaciones	Actualizar inventario de activos, inventariando y clasificando las grabaciones que contiene datos del titular de la tarjeta como confidencial, el CD utilizado para guardar esta información, bases de datos e informes que se envían al cliente también se deben clasificar como confidencial para generar el debido cifrамiento de esta documentación o fortalecer la herramienta como el uso de un SFTP o un FTPS. Utilizar siempre una empresa de envíos para enviar la información en el CD con esto se puede realizar un registro de seguimiento de este medio
9.6.3	Asegúrese de que la gerencia apruebe todos y cada uno de los medios que se trasladen desde un área segura (incluso, cuando se distribuyen los medios a personas).	No existe	No existe una aprobación formal de una dirección o la gerencia de la aprobación del medio utilizado para él envió de grabaciones que contiene datos del titular de la tarjeta, además de las debidas actividades de seguimiento que se deben realizar.	Se debe involucrar en el procedimiento de traslado de información la debida aprobación desde una dirección o desde la gerencia del transporte del CD, y que se realice un correcto seguimiento del medio.
9.7	**Lleve un control estricto del almacenamiento y la accesibilidad de los medios.**	No existe	Intercontact no guarda en medios externo información del titular de la tarjeta, solamente el CD que es enviado directamente al cliente, el resto de información es guardad en las base de datos, informes estadísticos, y grabaciones.	Se debe contar con un registro de todos los CD enviados al cliente para llevar a cabo su debido control. Llevar un debido control de inventario de los mismo como de igual manera el registro de transporte seguro de información
9.7.1	Lleve un registro detallado del inventario de todos los medios y lleve a cabo inventarios de los medios, al menos, una vez al año.	No existe	Intercontact no guarda en medios externo información del titular de la tarjeta, solamente el CD que es enviado directamente al cliente, el resto de información es guardad en las base de datos, informes estadísticos, y grabaciones.	Se debe contar con un registro de todos los CD enviados al cliente para llevar a cabo su debido control. Llevar un debido control de inventario de los mismo como de igual manera el registro de transporte seguro de información, este inventario se debe revisar estos erigirlos por lo menos una vez al año para su control

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
9.8	**Destruya los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales**	Definido	No se tiene medio físicos que contengan información del titular de la tarjeta, La compañía cuenta con un procedimiento de disposición final de medios removibles mediante un proceso de borrado seguro y un procedimiento de destrucción de documentación física.	Intercontact cuanta con procedimientos de disposición final de medios removibles y disposición final de documentos físicos. No se cuenta con medio físicos en la compañía que tengan información relacionada a los datos del titular de la tarjeta.
9.8.1	Corte en tiras, incinere o convierta en pulpa los materiales de copias en papel para que no se puedan reconstruir los datos del titular de la tarjeta. Proteja los contenedores de almacenamiento destinados a los materiales que se destruirán.	Definido	No se tiene medio físicos que contengan información del titular de la tarjeta, La compañía cuenta con un procedimiento de disposición final de medios removibles mediante un proceso de borrado seguro y un procedimiento de destrucción de documentación física.	Intercontact cuanta con procedimientos de disposición final de medios removibles y disposición final de documentos físicos. No se cuenta con medio físicos en la compañía que tengan información relacionada a los datos del titular de la tarjeta.
9.8.2	Controle que los datos del titular de la tarjeta guardados en medios electrónicos sean irrecuperables para que no se puedan reconstruir.	Definido	No se tiene medio físicos que contengan información del titular de la tarjeta, La compañía cuenta con un procedimiento de disposición final de medios removibles mediante un proceso de borrado seguro y un procedimiento de destrucción de documentación física.	Intercontact cuenta con procedimientos de disposición final de medios removibles y disposición final de documentos físicos. No se cuenta con medio físicos en la compañía que tengan información relacionada a los datos del titular de la tarjeta.
9.9	**Proteja los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones.**	No Aplicable	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada telefónica, estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada telefónica, estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.
9.9.1	Lleve una lista actualizada de los dispositivos. La lista debe incluir lo siguiente: Marca y modelo del dispositivo. Ubicación del dispositivo (por ejemplo, la dirección	No Aplicable	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada telefónica,	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	de la empresa o de la instalación donde se encuentra el dispositivo) Número de serie del dispositivo u otro método de identificación única		estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.	telefónica, estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.
9.9.2	Inspeccione periódicamente la superficie de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento)	No Aplicable	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada telefónica, estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada telefónica, estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.
9.9.3	Capacite al personal para que detecten indicios de alteración o sustitución en los dispositivos. La capacitación debe abarcar lo siguiente: Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de autorizarlos a acceder y modificar un dispositivo o solucionar algún problema. No instalar, cambiar ni devolver dispositivos sin verificación. Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por	No Aplicable	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada telefónica, estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.	Intercontact en la campaña de Metlife no realiza ningún tipo de transacción ni utiliza dispositivos físicos que utilicen la interacción directa con la tarjeta física. Lo único que realiza es la recolección de datos que se utilizaran para realizar debidos descuentos al usuario final mediante llamada telefónica, estos datos se envían directamente a Metlife que se encarga de realizar la transacción. En todo el proceso tampoco se recolecta datos como la clave o cualquier tipo de información confidencial de la tarjeta.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	ejemplo, a un gerente o encargado de seguridad).			
9.10	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.**	Repetible	Algunas políticas y procedimientos relacionados al acceso físico del personal externo están documentadas, aún faltan algunos aspectos por documentar.	Actualizar los procedimientos y políticas para el ingreso físico a las instalaciones, documentar todas las recomendaciones anteriormente descritas en los puntos anteriores.
Requisito 10	**Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta.**			
10.1	**Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.**	Inicial	Existen *logs* a nivel del directorio activo, no existen los a nivel de usuario en las aplicaciones en general, ni tampoco en la aplicación utilizada para la recolección de datos del titular de la tarjeta. No existen *logs* de auditoria de usuarios tampoco en el servidor de telefonía en el cual se loguean para realizar llamadas al usuario final y también es repositorio de grabaciones. No existen *logs* de auditoria en las bases de datos. Se desconoce si se tiene *logs* de auditorías en los aplicativos del cliente como es el FTP y la VPN site to client que se tiene con Intercontact.	Se debe configurar y habilitar la gestión de *logs* de los siguientes sistemas que a la fecha no se generan: -Aplicaciones web -Bases de datos -Servidor de Telefonía -Servidor de Aplicaciones -Servidor NAS Solicitar la cliente de Metlife que gestione los *logs* de los aplicativos que se tiene con Intercontact como son: -FTP -VPN Se debe garantizar que todos los accesos a los diferentes sistemas este vinculados usuarios específicos, no utilizar usuarios genéricos.
10.2	**implemente pistas de auditoría automáticas en todos los componentes del sistema a fin de reconstruir los siguientes eventos:**	Inicial	El directorio activo está configurado para que se generen *logs* de toda actividad de manera automática, estos *logs* son alojados en un repositorio debidamente identificado.	Configurar de manera automatizada la generación de los *logs* de los diferentes sistemas: -Aplicaciones web -Bases de datos -Servidor de Telefonía -Servidor de Aplicaciones

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
10.2.1	Todo acceso por parte de usuarios a los datos del titular de la tarjeta.	Inicial	El directorio activo es el único sistema configurado para que se generen *logs* de toda actividad de manera automática, estos *logs* son alojados en un repositorio debidamente identificado.	Se debe configurar todo el registro de los usuarios a los datos del titular en la tarjeta, se debe configurar el registro de todos los usuarios en los siguientes sistemas como mínimo: -Aplicaciones web -Bases de datos -Servidor de Telefonía -Servidor de Aplicaciones -Servidor NAS
10.2.2	Todas las acciones realizadas por personas con privilegios de raíz o administrativos	Inicial	Varios de los sistemas que están relacionados con el entorno de los datos del titular de la tarjeta aun no cuentan con registro de las acciones de cuentas administradoras o con privilegios de usuario *root* o sudo.	Se debe involucrar el registro de todas las cuentas de usuarios administradores de los sistemas, cuentas de usuario con privilegios de *root* o sudo.
10.2.3	Acceso a todas las pistas de auditoría	Inicial	El acceso a los *logs* del directorio activo está establecido para que solo sea posible por el administrador del sistema y nadie más tenga acceso para modificar consultar los *logs*. Cuando se ingrese a ver los *logs* de auditoria este acceso también tiene que ser registrado. No se tiene configurado los *logs* en otros sistemas.	Configurar los *logs* en los sistemas relacionados con el entorno de datos del titular de la tarjeta y que estos estén disponibles únicamente para las personas específicas como los administradores, para que estos registros no sean modificados por una persona malintencionada. El acceso a estos *logs* también debe quedar registrado.
10.2.4	intentos de acceso lógico no válidos	Inicial	Todos los *logs* incluidos el acceso lógico no valido quedan registrados en los *logs* del directorio activo. Se debe involucrar la configuración de los *logs* de los demás sistemas involucrados en el entorno de los datos del titular de la tarjeta y que registren los intentos de acceso lógico no validos	Configurar en todos los sistemas el registro de accesos lógicos no validos con el fin de identificar por ejemplo ataques de fuerza bruta.
10.2.5	Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.	No existe	No existe la configuración de *logs* que registren el aumento de privilegios en alguna cuenta. Tampoco se registra en ningún sistema el registro de la eliminación o creación de cuentas de usuario que cuenten con privilegios administrativos o raíz. En todos los sistemas si se tiene configurado sistemas de identificación y autenticación	Se deben configurar en todos los sistemas que tiene relación con el entorno de los de datos del titular de la tarjeta el registro de aumento de privilegios de alguna cuenta, la eliminación y creación de cuentas de usuarios que cuenten con privilegios administrativos o raíz.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
10.2.6	Inicialización, detención o pausa de los registros de auditoría	No existe	No existe la verificación de la inicialización, detención o pausa de los *logs* en ninguno de los sistemas	Se deben configurar en todos los sistemas que tiene relación con el entorno de los de datos del titular de la tarjeta la verificación de inicialización, detención o pausa de los *logs*. De igual manera restringir el acceso para que solo el administrador del sistema pueda ejecutar este tipo de actividad con el fin de que usuarios malintencionados realicen esta actividad.
10.2.7	Creación y eliminación de objetos en el nivel del sistema	No existe	En ningún sistema está configurado el registro de la creación y eliminación de objetos en el nivel del sistema.	Se deben configurar en todos los sistemas que tiene relación con el entorno de los de datos del titular de la tarjeta para que se registren todas las creaciones o eliminaciones de objetos a nivel del sistema, para evitar por ejemplo la instalación de algún tipo de *software* malicioso o *malware*. Se debe configurar por ejemplo registros en las bases de datos con el fin de identificar la creación o eliminación de tablas o procedimientos almacenados.
10.3	**Registre, al menos, las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:**	Inicial	Los únicos *logs* que se recolectan son los del directorio activo, inicio de sesiones, deslogueo, bloqueo de usuarios, creación y eliminación de cuentas entre otros, no se ha involucrado la configuración de *logs* en los demás sistemas.	Configurar en todos los sistemas registros de *logs* con el fin de identificar quien, que, como y cuando ingresaron a los sistemas o usaron servicios que estos proporcionan.
10.3.1	Identificación de usuarios	Inicial	Solo se identifica el registro de los usuarios que utilizan el directorio activo, inicio de sesiones en las estaciones de trabajo, no está configurado el registro de usuarios en los demás sistemas.	Configurar los registros en los siguientes sistemas que están relacionados con el entorno de los datos del titular de la tarjeta, estos deben identificar al usuario que utiliza cualquiera de los servicios o entran directamente al servidor -Aplicaciones web -Bases de datos -Servidor de Telefonía -Servidor de Aplicaciones -Servidor NAS

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
10.3.2	Tipo de evento	Inicial	Solo se identifica el tipo de evento el directorio activo, como es la creación de usuarios, inicio y deslogueo de sesiones, bloqueo de usuarios, entre otros. No está configurado el registro de usuarios en los demás sistemas.	Configurar los registros en los sistemas que están relacionados con el entorno de los datos del titular de la tarjeta, estos deben registrar los eventos clasificar estos como un tipo de evento especifico, Configurar estos registros en los siguientes sistemas: -Aplicaciones web -Bases de datos -Servidor de Telefonía -Servidor de Aplicaciones -Servidor NAS
10.3.3	Fecha y hora	Inicial	Solo se identifica la fecha y hora en los registros del directorio activo, No está configurado el registro de usuarios en los demás sistemas.	Configurar los registros en los sistemas que están relacionados con el entorno de los datos del titular de la tarjeta registros de entrada como fecha y hora Configurar estos registros en los siguientes sistemas: -Aplicaciones web -Bases de datos -Servidor de Telefonía -Servidor de Aplicaciones -Servidor NAS
10.3.4	Indicación de éxito o fallo	Inicial	Solo se identifica los registros que indican éxito o fallo en el logueo de usuarios, así como el bloqueo de cuentas en el directorio activo, No está configurado el registro de usuarios en los demás sistemas.	Configurar los registros en los sistemas que están relacionados con el entorno de los datos del titular de la tarjeta registros de entrada indicando el éxito o fallo, por ejemplo en el ingreso a algún servicio, servidor o aplicación. Configurar estos registros en los siguientes sistemas: -Aplicaciones web -Bases de datos -Servidor de Telefonía -Servidor de Aplicaciones -Servidor NAS
10.3.5	Origen del evento	No existe	No está configurado en ningún sistema el origen del evento	Configurar en todos los sistemas relacionados con el entorno de los datos del titular de la tarjeta el origen de los eventos en las entrada de registros

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
10.3.6	Identidad o nombre de los datos, componentes del sistema o recursos afectados.	No existe	No está configurado en ningún sistema el registro de entrada que identifique nombre, datos, componentes del sistema o recursos afectados	Configurar en todos los sistemas relacionados con el entorno de los datos del titular de la tarjeta la identidad o nombre de los datos, de los componentes del sistema o los recursos afectados.
10.4	**Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos.**	Definido	Está configurado para todos los sistemas una sincronización de relojes con la superintendencia y esta misma basa su hora con la hora atómica internacional UTC, los servidores de domino se sincroniza con este servidor NTP y todos los demás sistemas se sincronizan con el dominio. En algunos servidores con sistema operativos *Linux* no eran sincronizados los relojes	Se debe configurar la fecha y hora con algún servidor NTP o con el servidor de dominio como los otros servidores, los servidores que cuentan con S.O *Linux,* para que esta esté sincronizados como los otros sistemas
10.4.1	Los sistemas críticos tienen un horario uniforme y correcto.	Definido	Está configurado para todos los sistemas una sincronización de relojes con la superintendencia y esta misma basa su hora con la hora atómica internacional UTC, los servidores de domino se sincroniza con este servidor NTP y todos los demás sistemas se sincronizan con el dominio. En algunos servidores con sistema operativos *Linux* no eran sincronizados los relojes	Se debe configurar la fecha y hora con algún servidor NTP o con el servidor de dominio como los otros servidores, los servidores que cuentan con S.O *Linux*, para que esta esté sincronizados como los otros sistemas
10.4.2	Los datos de tiempo están protegidos.	Definido	A nivel de las estaciones de trabajo está bloqueado la configuración o cambio de la hora o fecha, solo con una cuanta administradora es posible realizar este cambio, los mismo a nivel ser servidores.	Verificar que esta configuración este aplicada a todos los servidores de la compañía. Configurar todos los sistemas para que registren en sus *logs* de eventos los cambios en la configuración de la hora y estos se supervisen y revisen
10.4.3	Los parámetros de la hora se reciben de fuentes aceptadas por la industria.	Definido	Los sistemas de la compañía están configurados con el servicio NTP de la superintendencia de industria y comercio, en el servidor de domino y el resto de servidores sincroniza la hora con estos servidores. Los servidores con sistema Operativo en *Linux* no tiene su hora sincronizada con un sistema NTP fiable	Se debe configurar la fecha y hora con algún servidor NTP o con el servidor de dominio como los otros servidores, los servidores que cuentan con S.O *Linux*, para que esta esté sincronizados como los otros sistemas

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
10.5	**Proteja las pistas de auditoría para que no se puedan modificar.**	Inicial	A nivel de directorio activo solo el administrador puede manipular los *logs* del sistema. No existe configuración de pistas de auditoria en los demás sistemas	Configurar los *logs* de auditoria en los demás sistemas que están relacionados con el entorno de los datos de la tarjeta, en las configuraciones deben establecer parámetros ara que estos *logs* estén protegidos, sean seguros y no se puedan modificar
10.5.1	Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales.	Inicial	A nivel de directorio activo solo el administrador puede manipular los *logs* del sistema. Es necesario ingresar al directorio activo como administrativo para visualizar estos *logs*. No existe configuración de pistas de auditoria en los demás sistemas	Configurar los *Backups* de los *logs* del directorio activo para que solo sean visibles por el administrador del sistema ya que este *backup* también se guarda otro servidor. Cuando se configure los demás sistemas para que generen *logs* de auditoria se debe limitar la visualización de estos *logs* solo a funcionario que por cuestiones laborales necesitan visualización de los mismos.
10.5.2	Proteja los archivos de las pistas de auditoría contra modificaciones no autorizadas.	Inicial	Existe una segmentación de red solo para los servidores A nivel de directorio activo solo el administrador puede manipular los *logs* del sistema, realizar modificaciones, eliminar, etc. Es necesario ingresar al directorio activo como administrativo para realizar estas modificaciones. No existe configuración de pistas de auditoria en los demás sistemas	Cuando se configure los demás sistemas para que generen *logs* de auditoria se debe proteger estos *logs* contra modificaciones no autorizadas incluyendo mecanismos de control de acceso.
10.5.3	Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.	Inicial	Dado que solo se realiza *logs* de auditoria en el directorio activo, solo se realiza un backup de estos, este *backup* se realiza en el mismo servidor y está configurado para que de manera automática se realice en el servidor NAS	Configurar los *backups* de los *logs* del directorio activo para que solo sean visibles por el administrador del sistema ya que este *backup* también se guarda otro servidor y este servidor el proporcionado por un proveedor externo y este también tiene acceso al servidor. Esta configuración también debe aplicar en los demás sistemas que se configuren para que proporcione *logs* de auditoria. La configuración de los backups también se recomienda que se realice de manera automática como los del directorio activo y en servidores de registros centralizados y que estén configurado para que estos sean difíciles de alterar.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
10.5.4	Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado.	No existe	No se guardan los registros para equipos como el *Firewall* y el servidor DMZ	Se recomienda guardar los *logs* de estos equipos que tienen acceso a rede externas la copia de sus registros en un servidor centralizado como el servidor NAS para evitar riesgo de pérdida o modificación
10.5.5	Utilice el *software* de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).	No existe	No existe ningún tipo de *software* que genere supervisión de integridad de archivos o detección de cambios en los registros	Se recomienda utilizar técnica para garantizar la integridad de los archivos o la detección de los cambios en los registro, por ejemplo el uso de *hash* en el archivo de *logs* este puede ser con SHA1 o superior o utilizar herramientas como: Algunas de las soluciones comerciales (licenciadas) que proporcionan monitorización de integridad son las siguientes: •*TripWire File Integrity Monitor* •*McAfee Integrity Control* •*CimTrak File Integrity Monitoring* •*Qualys* •*NetWrix Auditor* •*Verisys File Integrity Monitoring system* O soluciones *open source* como: •OSSEC •Samhain + Beltane •Integrit •AIDE •AFICK
10.6	**Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas.**	No existe	No se realizan revisiones regulares de los registros realizados	Se recomienda la implementación de herramientas para el análisis de registros como un SIEM como un OSIM, la instalación de un IDS por ejemplo un *Snort*, realizar la configuración de políticas y alertas en estos dispositivos para hacer revisiones más adecuadas.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
10.6.1	Revise las siguientes opciones, al menos, una vez al día: Todos los eventos de seguridad. Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD Registros de todos los componentes críticos del sistema. Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, *firewalls*, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).	No existe	No se revisan los eventos de seguridad, los registros de datos del titular, ni datos confidenciales de autenticación, tampoco los registros de todos los componentes críticos del sistema y registros de los servidores que realizan funciones de seguridad	Se debe implementar políticas o procedimientos que establezca la revisión al menos una vez al día los eventos de seguridad, los registros de datos del titular, datos confidenciales de autenticación, registros de todos los componentes críticos del sistema y registros de los servidores que realizan funciones de seguridad, ya sea con herramientas manuales de registro. Este monitoreo se puede realizar con una herramienta de correlacionador de eventos.
10.6.2	Revise los registros de todos los demás componentes del sistema periódicamente, de conformidad con la política y la estrategia de gestión de riesgos de la organización y según lo especificado en la evaluación anual de riesgos de la organización.	No existe	No este definidos por políticas o procedimientos las revisiones periódicas de los registros de todos los demás componentes del sistema	Definir por políticas o procedimientos las revisiones periódicas de los registros de los demás componentes del sistema de acuerdo con la evaluación de riegos detectados en la organización
10.6.3	Realice un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión.	No existe	No se realiza seguimiento de anomalías o excepciones dado que no existe un proceso definido de revisión de los registros del sistema	En las políticas o procedimientos se debe establecer actividades para realizar los debidos seguimientos de las excepciones y anomalías detectadas en el proceso de revisión.
10.7	**Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para**	No existe	No se tiene establecido políticas o procedimientos que establezcan la retención de registros de auditoria.	establecer políticas o procedimientos que establezcan la retención de registros de auditoria por lo menos un año,

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	la realización de copias de seguridad).			
10.8	**Requisitos adicionales solo para los proveedores de servicios: Implementar un proceso para la detección oportuna y la presentación de informes de fallas de los sistemas críticos de control de seguridad, incluido pero no limitado a la falla de: *Firewalls* IDS/IPS FIM Antivirus Controles de acceso físicos Controles de acceso lógico Mecanismos de registro de auditoría Controles de segmentación (si se utilizan)**	Inicial	Esta establecido un procedimiento establecido para reportar incidentes tanto de seguridad, como un procedimiento de incidentes de indisponibilidad o fallas en todos los sistemas de Intercontact	Como se había nombrado antes se recomienda instalar una herramienta para la detección oportuna de eventos como un correlacionador de eventos para la detección oportuna de cualquier tipo de incidente.
10.8.1	Requisitos adicionales solo para los proveedores de servicios: Responder a las fallas de los controles de seguridad críticos en el momento oportuno.	Definido	Esta establecido un procedimiento establecido para reportar incidentes tanto de seguridad, como un procedimiento de incidentes de indisponibilidad o fallas en todos los sistemas de Intercontact. Existe procedimiento de gestión de incidentes de seguridad y procedimiento de gestión de incidentes tecnológicos, estos procedimientos cuentan con aspectos como causa de la falla, implementación de controles para que esto no vuelva a ocurrir, entre otros	Incluir en el formato por procedimiento de incidencia la restauración de funciones de seguridad, realizar evaluación de riesgos para determinar si se requiere más acciones como resultado de la falla de seguridad.
10.9	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para**	Inicial	No existen políticas o procedimientos establecidos que establezca el monitoreo de todos los recursos de la red y los datos del titular. Existen informes mensuales de las diferentes plataformas que muestran varios aspectos de seguridad como son los accesos con que cuenta el sistema, alertas, eventos, entre otros.	Establecer una política que indique el monitoreo de todos los accesos a los recursos de la red y a los datos del titular de la tarjeta. Esta política debe divulgar y debe ser de conocimiento de todas las partes afectadas.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	todas las partes afectadas.			
Requisito 11	**Pruebe con regularidad los sistemas y procesos de seguridad**			
11.1	**Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados.**	No existe	No existen políticas ni procedimientos que defina la revisión trimestralmente puntos de accesos inalámbricos autorizados y no autorizados. Intercontact cuenta con políticas de usos de dispositivos móviles y además cuenta con el bloqueo de dispositivos removibles como USB y celulares a las estaciones de trabajo.	Implementar políticas o procedimientos que defina la revisión trimestralmente puntos de acceso inalámbrico autorizado y no autorizados. Se pueden incluir los métodos como análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos configurando las respectivas alertas. Se debe incluir al menos lo siguiente: *Tarjetas WLAN insertadas en los componentes del sistema *Dispositivos portátiles o móviles conectados a los componentes del sistema para crear puntos de acceso inalámbricos (por ejemplo, mediante USB, etc.). *Dispositivos inalámbricos conectados a un puerto o a un dispositivo de red.
11.1.1	Lleve un inventario de los puntos de acceso inalámbricos autorizados que incluyan una justificación comercial documentada.	Definido	Se tiene un inventario de activos en Intercontact que define el activo, propietario, clasificación, entre otros aspectos, allí de inventare los únicos puntos de acceso autorizados o *Acces point*.	Verificar que el inventario de activos se mantenga actualizado.
11.1.2	Implemente procedimientos de respuesta a incidentes en caso de que se detecten puntos de acceso inalámbricos no autorizados.	Definido	Se cuenta con un procedimiento de gestión de incidentes de seguridad en los cuales se establece que la violación de políticas de seguridad como un incidente de seguridad, dentro de las políticas de seguridad está incluida la política de uso dispositivos móviles y el uso aceptable de los activos.	Involucrar de manera específica en el uso de dispositivos móviles la prohibición de generar puntos de acceso inalámbricos no autorizados.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
11.2	**Realice análisis internos y externos de las vulnerabilidades de la red, al menos, trimestralmente y después de cada cambio significativo en la red (como por ejemplo, la instalación de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de *firewall*, actualizaciones de productos).**	Inicial	En intercontact se realiza análisis de vulnerabilidades semestralmente a los componentes de infraestructura tecnológica, no se tiene establecido un análisis de vulnerabilidades cuando se realice cambios significativos en la red.	Actualizar los indicadores de seguridad indicando que los análisis de vulnerabilidades ejecutados semestralmente, se ejecuten trimestralmente y que también se realicen después de un cambio significativo de la red.
11.2.1	Realice análisis interno de vulnerabilidades trimestralmente. Aborde las vulnerabilidades y realice redigitalizaciones para verificar que todas las vulnerabilidades de "alto riesgo" se resuelven de acuerdo con la clasificación de la vulnerabilidad de la entidad (según el Requisito 6.1). Los análisis deben estar a cargo de personal calificado.	Inicial	En intercontact se realiza análisis de vulnerabilidades semestralmente a los componentes de infraestructura tecnológica, cuando las vulnerabilidades clasificadas en niveles alto o critico se soluciona se realiza un retest verificando la debida solución de las mismas. Las vulnerabilidades son ejecutadas por una entidad externo por su defecto por el oficial de seguridad informática.	Actualizar los indicadores de seguridad indicando que los análisis de vulnerabilidades ejecutados semestralmente, se ejecuten trimestralmente y que se incluya un proceso la repetición de los análisis para verificar que se hayan solucionado todas las vulnerabilidades clasificadas con alto riesgo.
11.2.2	Los análisis trimestrales de vulnerabilidades externas deben estar a cargo de un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC (PCI Security Standards Council). Vuelva a realizar los análisis cuantas veces sea necesario hasta que todos los análisis estén aprobados.	Inicial	El análisis de vulnerabilidades cuando se ha realizado con un ente externo, se ha verificado que la empresa tiene larga trayectoria en el mercado, pero no se ha verificado si es un proveedor aprobado de escaneo que este certificado por el PCI-DSS.	Verificar que el asesor externo que realiza el análisis de vulnerabilidades externas cumple con los siguientes requisitos: "*Requerimientos de negocio: En los cuales se evalúa la estabilidad, independencia y cubrimiento por parte de pólizas de seguro de la empresa.* *Requerimientos de capacidad: En los que se revisa la experiencia de la empresa y del encargado de realizar los escaneos (scanning operation technical manager).* *Requerimientos administrativos: En la que se revisa si se cuenta con la logística necesaria para ejecutar los escaneos, incluyendo verificación de antecedentes, cumplimiento*

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
				con los procedimientos del PCI SSC, controles de calidad y protección de información confidencial y sensitiva proveniente de los resultados del ejercicio. Requerimientos para el mantenimiento de la certificación: En los cuales se definen los criterios anuales a ser cumplidos para mantener la credencial por parte de la empresa." *Tomado de www.pcihispano.com* Estos análisis deben ser ejecutados semestralmente y repetir los análisis con el fin de verificar que se haya cumplido con los requisitos de la guía del programa de ASV.
11.2.3	Lleve a cabo análisis internos y externos, y repítalos, según sea necesario, después de realizar un cambio significativo. Los análisis deben estar a cargo de personal calificado.	No existe	No se realiza análisis de vulnerabilidades cuando existen cambios significativos en la infraestructura tecnológica o red.	Realizar análisis de vulnerabilidades cuando se realicen cambios significativos a nivel de infraestructura o red o el análisis de los componentes del sistema que haya tenido cambios significativos.
11.3	**Implemente una metodología para las pruebas de penetración que incluya lo siguiente: Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800-115). Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. Incluya pruebas del entorno interno y externo de la red. Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. Defina las pruebas de penetración de la**	No existe	En Intercontact solo se realizan análisis de vulnerabilidades mas no se realizan pruebas de *pentest*.	Se deben realizar pruebas de *pentest* en la infraestructura relacionada al entorno de los datos de la tarjeta, estas pruebas de *pentest* deben cumplir con enfoques de *pentest* aceptados por la industria como por ejemplo basarse en la norma NIST SP800-115 Guía técnica de pruebas de seguridad de la información y evaluación. Se debe incluir pruebas a nivel interno y externo de red, pruebas en la capa de aplicación, capa de red, sistemas operativos, También se debe incluir la revisión y la evaluación de las amenazas y vulnerabilidades ocurridas o detectada en los últimos 12 meses. Documentar todos los resultados de las pruebas de *pentest* y las actividades de corrección de los mismos.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5. Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos. Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección.			
11.3.1	Lleve a cabo pruebas de penetración externas, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno).	No existe	En intercontact no se llevan a cabo pruebas de *pentest*	Se deben ejecutar pruebas de *pentest* externas por lo menos una vez al año y después de implementar un cambio o actualización significativa en la infraestructura o aplicaciones relacionadas con el entorno de datos del titular de la tarjeta. Este proceso lo debe ejecutar personal calificado ya sea escogido a nivel interno o ejecutado por una entidad externa Documentar políticas o procedimientos con el fin de establecer formalmente el procedimiento y que sea medible y revisado.
11.3.2	Lleve a cabo pruebas de penetración internas, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o	No existe	En intercontact no se llevan a cabo pruebas de *pentest*	Se deben ejecutar pruebas de *pentest* internas por lo menos una vez al año y después de implementar un cambio o actualización significativa en la infraestructura o aplicaciones relacionadas con el entorno de datos del titular de la tarjeta. Este proceso lo debe ejecutar personal calificado ya sea escogido a nivel interno o ejecutado por una entidad externa Documentar políticas o

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	un servidor web al entorno).			procedimientos con el fin de establecer formalmente el procedimiento y que sea medible y revisado.
11.3.3	Las vulnerabilidades de seguridad detectadas en las pruebas de penetración se corrigen, y las pruebas se repiten para verificar las correcciones.	No existe	En intercontact no se llevan a cabo pruebas de *pentest*	Cuando se detecten vulnerabilidades en las pruebas de *pentest* internas o externas ejecutadas, estas se deben solucionar y se deben repetir las pruebas con el fin de verificar la respectiva corrección.
11.3.4	Si se usa la segmentación para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes, realice pruebas de penetración, al menos, una vez al año y después de implementar cambios en los métodos o controles de segmentación para verificar que los métodos de segmentación sean operativos y efectivos, y que aíslen todos los sistemas fuera de alcance de los sistemas dentro del alcance.	No existe	En intercontact no se llevan a cabo pruebas de *pentest*. Se realiza segmentación de la red de Metlife para que este quede aislada, pero la red donde está el analista de calidad y de estadística no están debidamente segmentadas, la red de servidores también esta segmentada, pero estos servidores prestan servicios a varias campañas	Se debe ejecutar segmentación en las redes para aislar el entorno de datos del titular de la tarjeta, se recomienda trasladar a la red de Metlife al persona de estadística y analista de calidad para aislarlos de otras redes, lo mismo se recomienda aislar de manera lógica los servidores que prestan servicios de Metlife de otras campañas o implementar la autenticación de múltiples factores, ya sea al iniciar sesión en la red del CDE o al iniciar sesión en un sistema. Luego de esto realizar pruebas de *pentest* con el fin de validar y verificar que todos estos procesos de segmentación o controles son operativos y eficaces y que realmente si se está aislado de alguna manera los entornos de los datos del titular de la tarjeta del resto de entornos.
11.3.4.1	Requisitos adicionales solo para los proveedores de servicios: Si se utiliza la segmentación, confirme el alcance de la PCI DSS al realizar pruebas de penetración en los controles de segmentación al menos cada seis meses, y después de cualquier cambio a los controles/métodos de segmentación	No existe	En intercontact no se llevan a cabo pruebas de *pentest*	Realizar pruebas de *pentest* con el fin de validar y verificar que todos estos procesos de segmentación o controles son operativos y eficaces y que realmente si se está alineados de alguna manera los entornos de los datos del titular de la tarjeta del resto de entornos. Estas pruebas se deben ejecutar al menos cada seis meses o después de cualquier cambio significativo.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
11.4	**Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Monitoree todo el tráfico presente en el perímetro del entorno de datos del titular de la tarjeta y en los puntos críticos del entorno de datos del titular de la tarjeta, y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores de intrusión-detección y de prevención, las bases y firmas.**	Inicial	Intercontact cuenta con un *firewall* Fornitet que tiene incluido entre sus características un IPS, este se configura en varias de las políticas.	Instalar un dispositivo IDS como por ejemplo un Snort y configurar las diferentes reglas para detectar las diferentes amenazas que se presenten en el perímetro del titular de la tarjeta y generar las respectivas alertas. Estos sistemas se deben actualizar con frecuencia las bases y firmas. Este dispositivo debe ser instalado en un lugar que pueda monitorear todo el perímetro y puntos críticos del entorno de datos del titular de la tarjeta. Verificar que las políticas de IPS configuradas en el *firewall* cubran el entorno de datos del titular de la tarjeta.
11.5	**Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de integridad de archivos) para alertar al personal sobre modificaciones (incluyendo cambios, adiciones y eliminaciones) no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y configure el *software* para realizar comparaciones de archivos críticos, al menos, una vez por semana.**	No existe	No existe ningún tipo de *software* que genere supervisión de integridad para alertar al personal sobre las modificaciones	Se recomienda utilizar técnicas para garantizar la integridad de los archivos críticos del sistema, archivos de configuración o de contenidos por ejemplo con el uso de hash en el archivo de *logs* este puede ser con SHA1 o superior o utilizar herramientas como: Algunas de las soluciones comerciales (licenciadas) que proporcionan monitorización de integridad son las siguientes: *TripWire File Integrity Monitor McAfee Integrity Control CimTrak File Integrity Monitoring Qualys NetWrix Auditor Verisys File Integrity Monitoring system* O soluciones *open source* como: OSSEC Samhain + Beltane Integrit AIDE AFIC Se debe ejecutar por lo menos una vez por semana mediante el *software* la comparación de archivos críticos. Actualizar políticas o procedimiento en busca de formalizar este procedimiento.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
11.5.1	Implemente un proceso para responder a las alertas que genera la solución de detección de cambios.	No existe	No existe ningún tipo de *software* que genere supervisión de integridad para alertar al personal sobre las modificaciones	Actualizar el procedimiento de gestión de cambios o las políticas con el fin de involucrar el proceso para responder a las alertas que se generen en las herramientas implementadas para controlar los cambios.
11.6	**Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.**	Inicial	Existen procedimientos que establecen la ejecución de análsis de vulnerabilidades, se mide la solución de las mismas de acuerdo a uno indicadores de cumplimiento	Actualizar los procedimientos y políticas relacionadas a los puntos de acceso inalámbrico, análisis de vulnerabilidades y pruebas de *pentest* como lo establece la norma.
Requisito 12	**Mantenga una política que aborde la seguridad de la información para todo el personal**			
12.1	**Establezca, publique, mantenga y distribuya una política de seguridad.**	Definido	Intercontact cuenta con una política general y específica de seguridad de la información que aplica a todos los funcionarios, proveedores y terceros de la compañía. Esta política es de conocimiento y publicada a todos los interesados e involucrados	Verificar si los proveedores, contratistas o terceros nuevos de la compañía tienen conocimiento de las políticas de seguridad de la compañía.
12.1.1	Revise la política de seguridad, al menos, una vez al año y actualícela cuando se realicen cambios en el entorno.	Definido	Por políticas está establecido la revisión de todas las políticas de seguridad por lo menos una vez por semestre con el fin de actualizarlas o realizar cambios si cambia algo en el entorno	Verifique que las políticas hayan sido revisadas y exista evidencia física o digital de esto.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.2	**Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente: Se realiza, al menos, una vez al año y después de implementar cambios significativos en el entorno (por ejemplo, adquisiciones, fusiones o reubicaciones, etc.). Identifica activos críticos, amenazas y vulnerabilidades. Los resultados en un análisis formal y documentado de riesgo.**	Definido	Existe un procedimiento de gestión de riesgos en los cuales se detecta, evalúa, gestiona y trata todos los riesgos en seguridad de la compañía mediante una matriz de riesgos en un aplicativo desarrollado inhouse. Este análisis de riesgo es dinámico es decir que se actualiza cada vez que se detecta un nuevo riesgo o un riesgo existente cambia, la medición de estos riesgos se realiza de manera anual.	Identificar que el tratamiento de riegos y la evaluación de los riesgos se esté realizando de acuerdo al procedimiento establecido.
12.3	**Desarrolle políticas de uso para las tecnologías críticas y defina cómo usarlas correctamente.**	Definido	Intercontact tiene establecido políticas de seguridad en las cuales alguna de ellas involucran el uso de tecnologías especificas entre las cuales están: Política de uso de dispositivos móviles Política de teletrabajo Política de uso aceptable de los activos Política de control de acceso a la información Política de controles criptográficos y llaves criptográficas Política de claves Política de respaldo de información Política de trasferencia de información Política de adquisición, desarrollo y mantenimiento de *software* Política de gestión de cambios Política de acceso a internet Política de Antivirus Política de Correo	Actualizar las políticas de seguridad de uso de dispositivos móviles con aspectos relacionados con las laptos
12.3.1	Aprobación explícita de las partes autorizadas	Definido	Está definido por cumplimientos normativos relacionados a la ISO27001 revisar las políticas de seguridad son revisadas y aprobadas cada vez que se generen un cambio sobre estas. Cuando se implementan nuevas políticas estas son aprobadas por la alta dirección después de su debida revisión y análisis	Cada vez que sean aprobadas y actualizadas las políticas de seguridad estas deben ser informadas a todos los funcionarios y partes interesadas para ejercer el debido cumplimiento de las mismas

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.3.2	Autenticación para el uso de la tecnología	Definido	INTERCONTACT cuenta con políticas de control de acceso, política de controles criptográficas y llaves criptográficas, política de claves y política de teletrabajo que establecen métodos de autenticación para el uso de la tecnología	Identificar si se requiere la implementación de otros métodos de autenticación en las políticas por ejemplo el uso de tokens, dependiendo de la tecnología o a la información a la que se requiere acceder
12.3.3	Lista de todos los dispositivos y el personal que tenga acceso	Inicial	La compañía cuenta un inventario de activos de información donde están involucrado todos los dispositivos críticos y en general que contengan información de la empresa y del cliente. Solo esta listado el personal que tiene dispositivos móviles con información confidencial. Esta inventariado todas las MAC de los dispositivos que son conectados a la red inalámbrica	Verificar si todos los dispositivos están listados en el inventario de activos con su debida clasificación. Se debe listar todo el personal autorizado para utilizar los dispositivos y este debe ser revisado y actualizado con frecuencia.
12.3.4	Método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetado, codificación o inventario de dispositivos).	Definido	Está definido el procedimiento de inventario de activos y clasificación de la información. Toda la información de la compañía esta debida clasificada. El inventario de activos tiene campos como ID de activo, nombre, clasificación, dueño y ubicación	Se debe actualizar periódicamente el inventario de activos, además de agregar campos como por ejemplo propietario y contacto cuando aplique. Se debe identificar el uso de equipos o dispositivos que no estén debidamente etiquetados e inventariados. Se sugiere emplear un etiquetado lógico con el cual se determine con el código aspectos como: tipo de dispositivo, propietario, tipo de información, etc.
12.3.5	Usos aceptables de la tecnología	Inicial	Existen políticas de seguridad en la compañía , en alguna se involucra el uso aceptable de las tecnologías	Verificar las políticas de seguridad de la Información e involucrar en las que se crea pertinente el uso aceptable de la tecnología.
12.3.6	Ubicaciones aceptables de las tecnologías en la red	Inicial	Existen políticas de seguridad en la compañía, no se evidencia en las políticas de seguridad que se involucre las ubicaciones aceptables de la tecnología de red.	Completar las políticas de seguridad existentes involucrando en las políticas relacionadas a uso de dispositivos móviles y de red la definición de las ubicaciones aceptables de la tecnología en la red.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.3.7	Lista de productos aprobados por la empresa	No existe	No se identifica que en las políticas de seguridad de la compañía este una lista de productos aprobados por la empresa.	Se debe involucrar en las políticas de seguridad de Intercontact se incluya una lista de los productos aprobados por la empresa, identificado la tecnología aprobada por la compañía, con el fin de asegurar que no se abran brechas de seguridad.
12.3.8	Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad	Inicial	Las sesiones de las estaciones de trabajo, de las aplicaciones web y de las VPN site to client otorgadas, utilizan periodos de desconexión luego de un tiempo de inactividad en las sesiones. Por ejemplo las sesiones de las estaciones de trabajo se desloguea luego de 3 minutos de inactividad.	Verificar en las políticas de teletrabajo, políticas de control de acceso a la información o política de desarrollo se involucre la desconexión automática de las sesiones en las tecnologías de acceso remoto después de un periodo específico de inactividad. Solicitar al cliente Metlife la desactivación de sesiones cuando pase un lapso de tiempo determinado de las aplicaciones como VPN y FTP
12.3.9	Activación de las tecnologías de acceso remoto para proveedores y socios de negocio sólo cuando sea necesario, con desactivación inmediata después de su uso	Inicial	Existe un procedimiento de solicitud de acceso a VPN y privilegios, en el cual se legaliza cuando un proveedor, cliente o tercero necesita acceso remoto a recurso de la compañía. Se involucra aspectos específicos como usuario, recurso solicitado y tiempo de caducidad.	Verificar si realmente se estas desactivando los servicios de acceso remoto inmediatamente después de su uso, puede suceder que se otorguen los permisos pero luego no se vuelva hacer gestión de los mismos. Se debe involucrar en las políticas de seguridad la activación de estos acceso remotos solo cuando se necesiten y que se desactiven automáticamente después de usarlas.
12.3.10	En el caso del personal que tiene acceso a los datos del titular de la tarjeta mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos del titular de la tarjeta en unidades de disco locales y en dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad comercial definida. Si existe una necesidad comercial autorizada, las políticas de uso deben disponer la protección	No existe	No se identifica en las políticas de seguridad de la información de Intercontact la prohibición de copiar, mover o almacenar los datos del titular de la tarjeta de discos locales y en dispositivos electrónicos extraíbles al acceder a dichos datos a través de tecnologías de acceso remoto. Aunque solo el personal de tecnología, el DBA y el proveedor de telefonía podrían tener acceso remoto a los datos del titular de la tarjeta	Se debe involucrar en las políticas de seguridad la prohibición de copiar, mover o almacenar los datos del titular de la tarjeta de discos locales y en dispositivos electrónicos extraíbles al acceder a dichos datos a través de tecnologías de acceso remoto. Verificar que las configuraciones en los sistemas realicen correctamente estos bloqueos.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	de los datos de conformidad con los requisitos correspondientes de las PCI DSS.			
12.4	**Asegúrese de que las políticas y los procedimientos de seguridad definan, claramente, las responsabilidades de seguridad de la información de todo el personal.**	Definido	Está involucrado en las políticas de seguridad de Intercontact las responsabilidades de seguridad dela información de los funcionarios, terceros y proveedores. Además en los perfiles de cada funcionario también se definen responsabilidades concretas en seguridad de la información.	Se deben actualizar las políticas de seguridad con aspectos anteriormente descritos y verificar el cumplimiento en los funcionarios, terceros y proveedores
12.4.1	Requisitos adicionales solo para los proveedores de servicios: La gerencia ejecutiva deberá establecer la responsabilidad de la protección de los datos del titular de la tarjeta y un programa de cumplimiento de la PCI DSS para incluir: Responsabilidad general de mantener el cumplimiento de la PCI DSS Definir un estatuto para el programa de cumplimiento de la PCI DSS y la comunicación a la gerencia ejecutiva	No existe	No se ha realizado ninguna documentación o asignación de responsabilidad general para el mantenimiento de cumplimiento de la PCI DSS	Se debe involucrar en las políticas o en los perfiles de los funcionarios relacionados con el entorno de los datos del titular la responsabilidad general de mantener el cumplimiento con la PCI DSS. La alta dirección debe generar un estatuto u objetivo de cumplimiento de la PCI DSS e informar esto a todos los directivos de la compañía sobre la responsabilidad general de mantener el cumplimiento de la norma en la compañía.
12.5	**Asigne a una persona o a un equipo las siguientes responsabilidades de administración de seguridad de la información:**	Definido	La compañía cuenta con dos roles específicos en seguridad e la Información, uno es el oficial de seguridad de la información y el otro el oficial de seguridad informática.	Existe el rol de oficial de seguridad de la Información que es un representante de la alta dirección y un rol de oficial de seguridad informático que está encargado de toda la seguridad a nivel tecnológico
12.5.1	Establezca, documente y distribuya las políticas y los procedimientos de seguridad.	Definido	Cuando se inicia en un nuevo rol o cargo dentro de la compañía, dentro de las funciones de su cargo existen responsabilidades y deberes específicos relacionados a la seguridad de la información, de igual manera existe una formación inicial en la compañía en la cual se explica las políticas de seguridad de información así como los procedimientos y conceptos. Existen ejercicios de retroalimentación que involucra	En algunos casos cuando un funcionario empieza en la compañía no se realiza la debida formación relacionada a aspectos de seguridad que debe tener en cuenta en su cargo específico. Se debe involucrar en la formación del cargo aspectos de cumplimiento con la seguridad de la información.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
			aspectos de seguridad de la información	
12.5.2	Monitoree y analice las alertas y la información de seguridad y comuníquelas al personal correspondiente.	Inicial	Existe un procedimiento de incidentes de seguridad de la información, en este procedimiento se soluciona todos los incidentes de seguridad detectados o informados. De igual manera existe un procedimiento de comunicación de eventos, debilidades e incidentes que detecten todos los funcionarios de la compañía	Se debe implementar sistemas de información que monitoree y analice alertas como es un correlacionador de eventos, IDS, etc. Estos dispositivos se deben configurar de manera que generen las debidas alertas y que estas sean analizadas y que sean comunicadas al personal que se hay asignado formalmente.
12.5.3	Establezca, documente y distribuya los procedimientos de escalamiento y respuesta ante incidentes de seguridad para garantizar un manejo oportuno y efectivo de todas las situaciones.	Inicial	Por la herramienta de *help Desk* o por correo se informa los debidos incidentes de seguridad y son escalados al oficial de seguridad.	Se debe completar el debido procedimiento de gestión de incidentes con los debidos escalamientos y de respuesta que debe ser realizado ante un incidente de seguridad para garantizar el manejo efectivo y oportuno de todas las situaciones.
12.5.4	Administre las cuentas de usuario, incluso las incorporaciones, eliminaciones y modificaciones.	Definido	En intercontact existe el procedimiento de creación, modificación y eliminación de cuentas de usuario, cada vez que una persona ingrese a laborar a la compañía, cambie de cargo o sea desvinculada debe cumplir con el debido procedimiento que es administrado por el proceso de tecnología.	Se debe documentar formalmente que roles específicos del área de tecnología están encargados de administrar las diferentes cuentas de usuario.
12.5.5	Monitoree y controle todo acceso a los datos.	Inicial	Aunque inicialmente al asignar el perfil de usuario se limitan las conexiones, acceso a la información o carpetas este no se monitorea de manera formal.	Se debe documentar y asignar formalmente la responsabilidad de monitorear y controlar el acceso a los datos del titular de la tarjeta. Se sugiere asignar este rol a alguno del *help desk* de tecnología
12.6	**Implemente un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de la importancia de la seguridad de los datos del titular de la tarjeta.**	Inicial	Aunque existe un programa de formación en seguridad de la información que se involucra aspectos como son el cumplimiento de políticas de seguridad, conceptos básicos de seguridad, procedimientos, entre otros; no se involucra formalmente la importancia de seguridad que se le debe dar a los datos del titular de la tarjeta.	En las formaciones iniciales y las de refuerzo se debe involucrar el cumplimiento de políticas y procedimientos de seguridad relacionados con los datos del titular de la tarjeta en cargos o roles que estén relacionados con el entorno de los datos del titular de la tarjeta

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.6.1	Capacite al personal inmediatamente después de contratarlo y, al menos, una vez al año.	Definido	Está definido los procedimientos de formación iniciales y formaciones de refuerzo que se realizan de manera semestral o anual según lo defina la compañía	En las formaciones iniciales y las de refuerzo se debe involucrar el cumplimiento de políticas y procedimientos de seguridad relacionados con los datos del titular de la tarjeta en cargos o roles que estén relacionados con el entorno de los datos del titular de la tarjeta
12.6.2	Exija al personal que realice, al menos, una vez al año, una declaración de que leyeron y entendieron la política y los procedimientos de seguridad de la empresa.	No existe	No existe una declaración formal de los empleados en el cual incluya que leyeron las políticas y procedimientos de seguridad de Intercontact. En las formaciones iniciales se realiza evaluaciones que evalúa algunos aspectos de seguridad explicados.	Se debe documentar formalmente una declaración por lo menos anual de los funcionarios de intercontact que incluya que leyeron y entendieron las políticas de seguridad de la compañía y están comprometidos con las mismas. Esta declaración puede ser de manera física o electrónica
12.7	**Examine al personal potencial antes de contratarlo a fin de minimizar el riesgo de ataques desde fuentes internas. (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias).**	Definido	Todos los funcionarios contratados en Intercontact se les han verificado antes de su contratación antecedentes por policía, procuraduría, referencias laborales, personales y de educación. No se les realiza verificaciones crediticias.	Verificar de manera formal que si se estén realizando todo el tipo de verificaciones que están establecidas por el procedimiento de gestión humana.
12.8	**Mantenga e implemente políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta**	Definido	En Intercontact cuenta con política de relación de proveedores, procedimientos de acceso a VPN y privilegios, acuerdos de confidencialidad, contratos, entre otros. Estos procedimientos y políticas deben ser de cumplimiento con los proveedores.	Se debe revisar que proveedores tiene acceso o se comparte información de datos del titular, por ejemplo *Mitrol y Losytec* verificar que estos estén cumpliendo con todas las políticas y procedimientos de la compañía y limitar el acceso a los datos en el mayor grado posible. Si por alguna estos no necesitan acceso se deben bloquear los permisos o cifrar la información para que este no pueda acceder.
12.8.1	Mantener una lista de proveedores de servicios, incluida una descripción del servicio prestado.	Definido	Intercontact cuenta con una lista de proveedores y que servicio ofrece cada proveedor a la compañía.	Verificar que la lista de proveedores se mantenga actualizada y que en todos se involucre una descripción del servicio prestado, cada vez que ingresa un proveedor nuevo o se elimine un proveedor, a algún dato cambie con este proveedor (razón social, procesos, etc.)

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.8.2	Mantenga un acuerdo por escrito en el que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente.	No existe	Intercontact solo tiene un acuerdo de confidencialidad con los proveedores pero no existe un acuerdo a nivel contractual que aceptan responsabilizarse por la seguridad de los datos del titular de la tarjeta.	Verificar que proveedores tiene acceso a los datos del titular de la tarjeta y establecer un acuerdo por escrito en el cual los proveedores aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos almacenan o procesan. Entre los proveedores identificados esta Mitrol (telefonía) y Losytec(Backups)
12.8.3	Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios, que incluya una auditoría adecuada previa al compromiso.	No existe	No existe ningún proceso de auditoria previa al contrato comercial con los proveedores, ni con los proveedores que en este momento tengan relación con el almacenamiento, procesamiento y trasferencia de información de datos del titular.	Involucrar un proceso de auditoria previa al compromiso con proveedores que van a tener relación con los datos del titular de la tarjeta (almacenamiento, procesamiento y transmisión) o con los proveedores que ya se tiene una relación comercial, eta auditoria debe evaluar aspectos como prácticas de presentación de informes, respuesta ante incidentes, detalles de cómo asignan responsabilidades de la PCI DSS, cumplimiento con la PCI DSS y que evidencias se presentaran.
12.8.4	Mantenga un programa para monitorear el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios.	No existe	No existe un procedimiento que monitorea el estado de cumplimiento de los proveedores con respecto a la PCI DSS	Se debe establecer un programa de monitoreo o auditoria de cumplimiento con la PCI DSS con todos los proveedores que tengan relación con los datos del titular de la tarjeta. Puede ser una tarea programada con cierta periodicidad.
12.8.5	Conserve información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad.	No existe	No está identificado que requisitos de la PCI DSS son administrados por el proveedor de servicios.	Primero se debe verificar que servicios ofrece cada proveedor que tenga relación con el almacenamiento, procesamiento o transmisión de información de datos del titular e identificar qué requisitos de la PCI DSS aplican a estos para determinar qué requisitos son administrados por Intercontact y cuales por el proveedor

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.9	**Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios aceptan, por escrito y ante los clientes, responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente.**	Definido	Intercontact cuenta con un contrato con la empresa Metlife, en el cual establecer acuerdos de confidencialidad, debido tratamiento de la información y las respectivas responsabilidades que tiene la empresa con el almacenamiento, procesamiento y transmisión de la información de datos del titular.	Verificar que la compañía si tiene por escrito mantener los requisitos correspondientes de la PCI DSS con Metlife
12.10	**Implemente un plan de respuesta ante incidentes. Prepárese para responder de inmediato ante un fallo en el sistema.**	Definido	Existe un procedimiento de gestión de incidentes de seguridad, un procedimiento de gestión de incidentes en plataformas o servicios tecnológicos y un plan de continuidad del negocio. Todos los incidentes detectados son informados por la línea de atención al *help desk* o por la plataforma de *help desk*	Se debe informar a los funcionarios o partes interesadas los procedimientos de gestión de incidentes que tiene intercontact para evitar periodos de inactividad más prolongados para el negocio, responsabilidades legales y exposición innecesaria de medios al publico
12.10.1	Desarrolle el plan de respuesta ante incidentes que se implementará en caso de que ocurra una falla del sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente: Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago. Procedimientos específicos de respuesta a incidentes. Procedimientos de recuperación y continuidad comercial. Procesos de copia de seguridad de datos. Análisis de los requisitos legales para	Repetible	En los procedimientos de gestión de incidentes no está documentado aspectos específicos como roles, responsabilidades, contacto en caso de riesgos, procedimientos específicos de respuesta a incidentes Por cultura organizacional todo se reporta la *Help Desk.* Si existe un documento de continuidad del negocio, políticas de copias de *backups.* No existe un análisis de los requisitos legales para el informe de riesgos. Se realiza un informe del incidente ocurrido.	Se deben documentar como se relacionan los procedimientos de gestión de incidentes de seguridad y gestión de incidentes en plataformas tecnológicas. Complementar en procedimiento de incidentes en los componentes tecnológicos incluyendo los siguientes aspectos cuando sea comprometido un sistema que esté relacionado con el entorno de los datos del titular: Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya Análisis de los requisitos legales para el informe de riesgos. Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
	el informe de riesgos. Cobertura y respuestas de todos los componentes críticos del sistema. Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago.			
12.10.2	Revise y pruebe el plan, incluidos todos los elementos enumerados en el Requisito 12.10.1, al menos anualmente.	Inicial	Existe un plan ante incidentes pero no está involucrado varios aspectos como son: Análisis de los requisitos legales para el informe de riesgos. Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago.	Involucrar en el plan de continuidad aspectos como: Análisis de los requisitos legales para el informe de riesgos. Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago.
12.10.3	Designe a personal específico para que esté disponible las 24 horas al día, los 7 días de la semana para responder a las alertas.	Definido	En intercontact están definidos tres niveles de atención las 24 horas del día los 7 dos de la semana: Nivel 1: Nivel de soporte, primer contacto ante la falla de algún componente de los sistemas Nivel 2: Infraestructura, es el segundo contacto en caso que el primer nivel no logre solucionar la incidencia Nivel 3: Nivel directivo que es contactado en caso que ninguno de los dos primeros niveles pueda solucionar la incidencia.	Involucrar en las políticas o en las funciones de los perfiles específicos del proceso de tecnología, la disponibilidad de funcionarios las 24 horas 7 días a la semana, entre las funciones también se debe incluir la respuesta ante incidentes, el monitoreo de la cobertura de cualquier evidencia de actividad no autorizada, detección de puntos de acceso inalámbricos no autorizados, alertas críticas de por ejemplo un IDS o informes de cambios no autorizados en archivos de contenido o de sistemas críticos.
12.10.4	Capacite adecuadamente al personal sobre las responsabilidades de respuesta ante fallas de seguridad.	Definido	Cuando ingresa un nuevo funcionario al proceso de tecnología se le explica sus funciones y responsabilidades ante el cargo donde se involucrar las responsabilidades, criterios de comunicación y respuestas que debe ejecutar ante alguna falla de seguridad.	Evidenciar de manera formal o documental que todos los funcionarios de tecnología fueron capacitados ante las responsabilidades, criterios de comunicación y respuestas que deben ejecutar ante alguna falla de seguridad, que están basados en los procedimientos de gestión de incidentes de seguridad y gestión de incidentes en plataformas o servicios tecnológicos

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.10.5	Incluya alertas de los sistemas de supervisión de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, *firewalls* y sistemas de supervisión de integridad de archivos.	Inicial	La únicas alertas que se generan las 24 horas son unas configuradas en la mayoría de los componentes tecnológicos para que sean reportados al Nagios	Implementar sistemas como IDS, IPS, smtp del *firewall* para que genere alertas al nagios y sistemas de integridad de archivos que genere alertas sobre los sistemas involucrados en el entorno de datos del titular de la tarjeta e involucre procedimientos de observación y revisión de estos sistemas y que los planes de respuesta ante incidentes se inicien cuando se presente un incidente. En los procedimientos documentados de gestión de incidentes se debe incluir la supervisión y respuesta a las alertas de seguridad
12.10.6	Elabore un proceso para modificar y desarrollar el plan de respuesta ante incidentes según las lecciones aprendidas e incorporar los desarrollos de la industria.	Inicial	Aunque el procedimiento de gestión de incidentes de seguridad tiene la parte de lecciones aprendidas con el fin de ejecutar procesos y actividades en busca de que no se vuelvan a repetir, esto no está involucrado en la gestión de incidentes en componentes tecnológicos	Involucrar en el procedimiento de gestión de incidentes en componentes de tecnología las lecciones aprendidas con el fin de ayuda a mantener el plan actualizado y a ser capaz de reaccionar ante las amenazas emergentes y las tendencias de seguridad.
12.11	**Requisitos adicionales solo para los proveedores de servicios: Realizar revisiones al menos trimestralmente para confirmar que el personal sigue las políticas de seguridad y los procedimientos operativos. Las revisiones deben cubrir los siguientes procesos: Revisiones del registro diario. Revisiones del conjunto de reglas de *firewall*. La aplicación de las normas de configuración a los nuevos sistemas. Respuesta a las alertas de seguridad. Procesos de gestión del cambio**	Definido	Existen auditorias de autocontrol internas y de seguimientos para todo el año, existen verificaciones mensuales que se realizan a los sistemas como políticas de seguridad a nivel de *firewall* y demás plataformas, cumplimiento con las políticas de seguridad de la compañía, evaluación de cambios que se realiza de manera semanal y análisis de vulnerabilidades	Se debe involucrar las revisiones de las alertas de seguridad de los sistemas que tiene relación con el entorno de los datos del titular al menos trimestralmente.

Cuadro 3. (Continuación)

Numeral	Requisito	Estado	Estado actual	Actividades a realizar
12.11.1	Requisitos adicionales solo para los proveedores de servicios: Mantener la documentación del proceso de revisión trimestral para incluir: Documentar los resultados de las revisiones Revisión y cierre de los resultados por el personal asignado a la responsabilidad del programa de cumplimiento de la PCI DSS	Inicial	Se tiene documentación auditorias de autocontrol internas y de seguimientos de todo el año, existen verificaciones mensuales que se realizan a los sistemas como políticas de seguridad a nivel de *firewall*, y demás plataformas cumplimiento con las políticas de seguridad de la compañía, evaluación de cambios que se realiza de manera semanal.	Se debe documentar las revisiones que se realiza sobre el sistemas sobre los procedimientos, configuraciones y políticas establecidos por la PCI DSS, esta documentación debe complementar la documentación que ya está llevando el sistema de gestión de seguridad de Intercontact
Fuente: Elaboración propia, 2017				

A continuación se muestra, el porcentaje de cumplimiento con relación a PCI-DSS y partiendo que para generar un debido cumplimiento de los controles de la norma deben estar en un estado Definido o Superior debido a que un control en un estado inferior significaría que no está documentado, incompleto o la implementación no es la adecuada. Ver Tabla 1.

Tabla 1. Estado actual de cumplimiento de controles de PCI-DSS

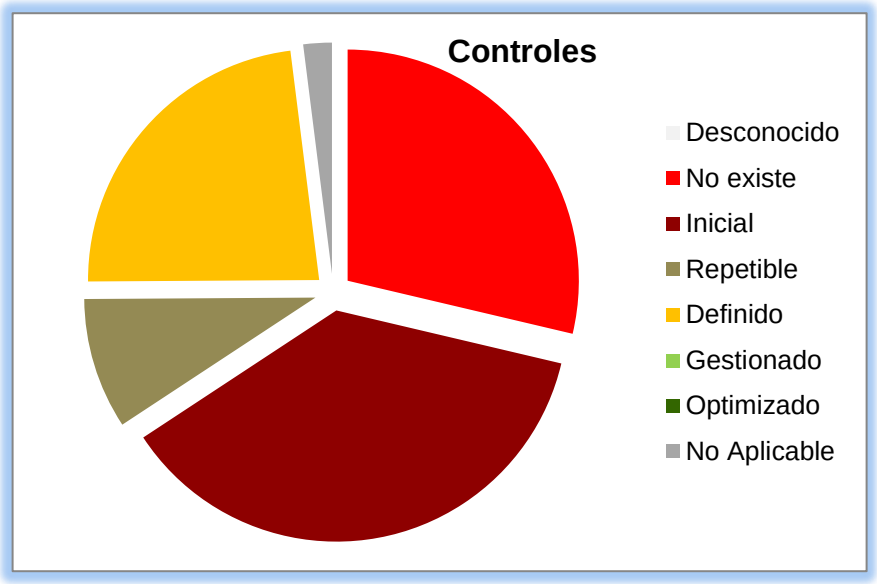
Estado	Significado	Porcentaje de los controles para el sistema de Información
Desconocido	No hay información suficiente para establecer el nivel de madurez	**0%**
No existe	No cuenta con el procedimiento o control definido por la norma.	**28.7%**
Inicial	Se reconoce la necesidad pero no se han identificado los mecanismos para implementar los controles	**37.1%**
Repetible	Se ejecutan los controles pero no están documentados, se depende de la disponibilidad del responsable del control para su ejecución	**9.2%**
Definido	El control está documentado, se ha divulgado, pero no se realizan mediciones de su desempeño	**23.1%**
Gestionado	Se han definido los límites dentro de los cuales debe operar el control, se evalúa el desempeño y se generan informes	**0%**

Tabla 1. (Continuación)

Estado	Significado	Porcentaje de los controles para el sistema de Información
Optimizado	Se incorporan las mejores prácticas de la industria y las métricas de los controles se consolidan en herramientas estratégicas de toma de decisiones, ejemplo Balance Score Card	**0%**
No Aplicable	Los controles no son aplicables a la actividad o proceso	**2.0%**

Fuente: Elaboración propia, 2017

Gráfica 1. Estado actual de cumplimiento de controles de PCI-DSS



Fuente: Elaboración propia, 2017

Como se observa, la mayoría de controles requeridos por la PCI-DSS están en un estado inicial, repetible o por defecto no existen, este porcentaje corresponde al 75% y tan solo el 23% de controles que están en un estado definido, esto quiere decir que el control está documentado, se ha divulgado pero no se realizan medidas de su desempeño. Ver Gráfica 1.

11. PLAN DE ACCIÓN

Con las actividades a realizar anteriormente descritas a lo largo de todo el análisis GAP se busca que la compañía INTERCONTACT logre llegar a un estado Definido con relación a los controles de la norma PCI-DSS, esto quiere decir que el control está documentado, se ha divulgado, pero no se realizan mediciones de su desempeño. De acuerdo a esto la compañía empezaría a realizar otras mejoras para Madurar en la implementación y cumplimiento de la PCI-CSS en la campaña Metlife y otras campañas que involucren el almacenamiento, transferencia y manejo de información del titular y de la tarjea.

Como se nombró con anterioridad el 75% de los controles están por debajo de un estado Definido y solo el 23% de los controles están definidos y solo un 2% de estos controles no aplican. Con este análisis GAP se dividieron todas las actividades en cinco grandes conjuntos para ser implementados, los cuales son Procedimientos, Actividades, Políticas, Recomendaciones y Adquisiciones o Compras. Con la finalidad de al ser implementadas dar cumplimiento a la PCI-DSS.

El plan de acción tendrá la siguiente estructura: Objetivo, Requerimientos cubiertos, Acciones, Recursos, Tiempo y Responsables. Sera dividido en los diferentes principios de la norma.

A continuación se muestra los planes de acción que debe ejecutar Intercontact para que pueda dar cumplimiento al objetivo planteado y los requerimientos de PCI-DSS.

11.1 INSTALE Y MANTENGA UNA CONFIGURACIÓN DE *FIREWALL* PARA PROTEGER LOS DATOS DEL TITULAR DE LA TARJETA

El plan de acción que se llevara a cabo para dar cumplimiento al requisito 1 de la PCI DSS se muestra a continuación. Ver Cuadro 4.

Cuadro 4. Instalar y mantener una configuración de *Firewall*

Objetivo	Mantener una configuración adecuada del *firewall* para proteger los datos del titular de la tarjeta.
Requerimientos Cubiertos	1.1 – 1.5
Acciones	▪ Crear procedimiento de la configuración del *firewall* para la implementación de campañas que almacenen, transfieran y procesen datos del titular de la tarjeta. Este procedimiento también debe involucrar configuraciones

Cuadro 4. (Continuación)

Acciones	que debe tener el *firewall* relacionado al servidor DMZ. También requerimientos mínimos para establecer una política en el *firewall* que de acceso a internet, tenga parámetros de NAT para evitar que las redes externas no sean visibles desde internet y documentar los pasos para realizar políticas de seguridad y conexiones, redes externas y todo lo relacionado para la administración del *firewall*. ▪ El procedimiento de gestión de cambios deben involucrar la aprobación y pruebas para cambios configurados en el *firewall*. ▪ Actualizar el diagrama de red que muestre detalles de la estructura tecnológica a nivel de red LAN (vlans, acls, redes inalámbricas, conexión a servidores, stacks, todos los dispositivos de red y demás), donde se documente todas las conexiones que existen entre los datos de los titulares de la tarjeta. ▪ Realizar diagramas de flujo de datos en el que se evidencie el flujo de datos de los titulares de las tarjetas donde se identifiquen parámetros como almacenamiento. ▪ El director de tecnología debe documentar descripción de roles y responsabilidades de quienes acceden al *firewall* y como otras más puntuales para el administrador de los dispositivos de red. ▪ Se debe definir y documentar todos los servicios, protocolos, puertos, rutas y demás de manera formal y justificada de cada campaña en especial la campaña de Metlife con las respectivas funciones de seguridad de cada servicio configurado. Asegurar que deshabiliten o eliminen el resto de los protocolos, servicios y puertos que no son necesarios para la ejecución normal de la campaña. ▪ Se debe realizar de manera formal y medible la revisión de las normas de configuración del *firewall* (políticas, rutas, webfilters, application control, puertos, etc) mínimo cada seis meses de las debidas campañas (Metlife) en comparación a la implementación o solicitud formal de la misma. ▪ Verificar que todas las conexiones a la fecha hacia redes no confiables o externas estén debidamente configuradas. ▪ Configurar la campaña Metlife para que se restringa la

Cuadro 4. (Continuación)

	cantidad necesaria de tráfico tanto entrante como saliente y documentar el mismo ▪ Se debe configurar el *firewall* para que separe la red de Metlife y la red inalámbrica, segmentar la red donde se aloja la base de datos y aplicaciones CDE. ▪ Se debe documentar todos los cambios que se realizan en el core y generar una tarea (*checklist*) en la que se guarde el archivo de configuración antes de sacar el *backup*. ▪ Garantizar que las redes internas que gestionan los datos de las tarjetas y titulares de las tarjetas tenga debidamente denegado o controlado el acceso a internet. ▪ La configuración de las aplicaciones montadas en la DMZ estén con la debida documentación, gestión de cambios y análisis de riesgos. ▪ Verificar que en la reglas de DMZ tenga definida en sus reglas que las direcciones internas no se pueden transferir de Internet a la DMZ. ▪ Se debe bloquear o limitar el acceso a internet los analistas de estadística y de calidad. ▪ Instalar un *firewall* personal a los equipos móviles corporativos como computadores portátiles, debe aplicar las políticas de seguridad y restricciones que se tiene dentro de las instalaciones de la compañía.
Recursos	Recurso humano, capacitación en normas como la NIST (*Guidelines on Firewalls and Firewalls Policy*)
Tiempo	2 Meses
Responsables	Administrador del *Firewall*, Director de Tecnología
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Se sugiere documentar los perfiles y permisos específicos de las redes que tratan los datos del titular de la tarjeta.
- Se recomienda tomar como base la guía para la debida configuración del *firewalls* la NIST- *Guidelines on Firewalls and Firewalls Policy - Recommendations of the National Institute of Standards and Technology - Karen Scarfone, Paul Hoffman.* Tener en cuenta aspectos como Políticas del *firewalls*

y Planificación e implementación.

- Para verificar si el *firewalls* cuenta con características de Stateful y contar con controles de *antispofing* como primera medida hay que identificar si esta versión de *Fortinet* tiene la funcionabilidad de *Stateful Packet Inspeccion* “SPI” o *Dynamic Packet Filtering*. Como siguiente opción se puede utilizar NMAP.

Para validar los controles de Anti-Spoofing:
NMap flags para validación de Anti-Spoofing

1- -S <IP_Address>: Spoof source address

2- -e <iface>: Use specified interface

Para validar las características de *Stateful Inspection:NMap flags* para validar *Stateful Inspection Shell*

1 -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans

2 -sN/sF/sX: TCP Null, FIN, and Xmas scans

3 --scanflags <flags>: Customize TCP scan flags

4 -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

PROCEDIMIENTOS

Aprobación y pruebas para cambios configurados en el *firewall*.

Cada vez que se vaya a configurar una campaña nueva se debe cumplir con el seguimiento y actividades que den cumplimiento a requisitos mínimos que deben ser configurados antes de su salida a producción. Se puede utilizar el siguiente formato para dar el debido cumplimiento. Ver Cuadro 5.

Cuadro 5. Formato de implementación de campaña

Objetivo: Realizar la entrega de todos los elementos necesarios para el inicio de las campañas solicitadas por el área de Operaciones o Administrativas

Fecha Solicitud_____No Solicitud en SD:_____
Campaña: :_____Fecha de Entrega:_____

Item	*Estado*	*Recibido*	*Observaciones de la entrega*
Enrutamientos Telefonía			
Creación de campaña Mi trol			
Creación de Agentes Mi trol			
Creación de Sesiones			
Acceso Panel de Control			
Acceso al CMD y Ejecutar			
Acceso Agregar Impresoras			
Acceso a Disco del SO			
Acceso al Reproductor de Windows			
Mitrol			
JAVA			
.Net Framework			
Avaya Softphone			
CMS			
Nice			
WFO			
Nov Observe			
MS Office			
Firefox			
Google Chrome			
Open Office			
Antivirus			
7 ZIP			
Communicator			
RR			
Avaya Workbar			
SAP			
CoolTimer			
Otros:			
Carpeta Compartida			
Segmento de Red (VLAN)			
Acceso a Aplicaciones consultadas de Internet o redes externas			
Accesos a Internet, Páginas WEB Especiales			
Bloqueo Internet o Páginas WEB no Autorizadas			
VPN site to site o SSL			
Rutas			
Puertos IN/OUT			

Cuadro 5. (Continuación)

Acceso a la red inalámbrica			
Configuración NAT en la política de Firewall			
Permisos especiales o excepciones (Indicar si algún perfil, funcionario o cliente necesita un requerimiento especial –Red, Internet, puerto, servicio, etc)			
ACL			
Acceso USB y Unidad CD			
Configuración Impresora			
Diademas			
Estaciones de trabajo funcionales			
Permite Instalación/Desinstalación de software?			
Observaciones: (En caso que se necesite utilizar ciertos servicios, puertos o funciones inseguras, este riesgo tiene que estar definido y debidamente tratado para que de esta manera se pueda utilizar estos privilegios de manera segura)			
ENTREGA DIRECTOR TECNOLOGÍA **FIRMA:** **NOMBRE:**		**RECIBE DIRECTOR DE OPERACIONES** **FIRMA:** **NOMBRE:**	

Fuente: Elaboración propia, 2017

Todas las solicitudes de cambios, actualizaciones o creaciones de campañas deben ser solicitadas al *service desk* con toda la documentación adjunta requerida, cuando es un caso puntual de igual manera debe ser solicitado al *service desk* y evaluado por los administradores. Además la revisión de las reglas de filtrado por lo menos cada seis (6) meses.

Se sugiere revisar todas las campañas y perfiles con el fin de garantizar permisos específicos de las redes que tratan los datos del titular de la tarjeta.

Se debe tener en cuenta configurar las políticas del *firewalls* de la siguiente manera. Ver Cuadro 6.

Cuadro 6. Configuración de *firewall*

Origen -> Destino	Tráfico permitido
De Internet a la DMZ PCI DSS	Únicamente a los puertos autorizados (Req. 1.3.1 y 1.3.2) empleando NAT (Req. 1.3.8). Activar funcionalidades de AntiSpoofing en el firewall (Req. 1.3.4)
De Internet a la red Interna PCI DSS	Todo el tráfico denegado (Req. 1.3.3)
De Internet a la red de gestión PCI DSS	Únicamente tráfico VPN administrativo autorizado con autenticación de dos factores (Req. 1.4, 8.3 y 12.3.10)
De Internet a la red inalámbrica	Todo el tráfico denegado (Req.1.2.3)
De la DMZ PCI DSS a la red Interna PCI DSS	Únicamente a los puertos autorizados (Req. 1.3.7)
De la DMZ PCI DSS a la red de gestión PCI DSS	Únicamente a los puertos autorizados (Req. 1.3.7)
De la DMZ PCI DSS a Internet	Únicamente a los puertos autorizados empleando NAT (Req. 1.3.5 y 1.3.8)
De la DMZ PCI DSS a la red inalámbrica	Todo el tráfico denegado (Req. 1.2.3)
De la red Interna PCI DSS a Internet	Todo el tráfico denegado (Req. 1.3.3, 1.3.5 y 1.3.7)
De la red Interna PCI DSS a la DMZ PCI DSS	Todo el tráfico denegado (Req. 1.3.5 y 1.3.7)
De la red interna PCI DSS a la red de gestión PCI DSS	Únicamente a los puertos autorizados (Req. 1.3.7)
De la red interna PCI DSS a la red inalámbrica	Todo el tráfico denegado (Req. 1.2.3 y 1.3.7)
De la red de gestión PCI DSS a Internet	Todo el tráfico denegado (Req. 1.3.3)
De la red de gestión PCI DSS a la DMZ PCI DSS	Únicamente a los puertos autorizados para efectos de administración y actualizaciones
De la red de gestión PCI DSS a la red interna PCI DSS	Únicamente a los puertos autorizados para efectos de administración (Req. 1.3.7)
De la red de gestión PCI DSS a la red inalámbrica	Únicamente a los puertos autorizados para efectos de administración
De la red inalámbrica a Internet	Todo el tráfico denegado (Req. 1.3.3)
De la red inalámbrica a la DMZ PCI DSS	Únicamente a los puertos autorizados (Req. 1.2.3)
De la red inalámbrica a la red de gestión	Todo el tráfico denegado (Req. 1.2.3)
De la red inalámbrica a la red interna PCI DSS	Todo el tráfico denegado (Req. 1.2.3)

Fuente: pcihispano.com

Configuración de Aplicaciones en la DMZ.

Dado que las aplicaciones a la fecha que están en la DMZ son aplicaciones que han estado en producción a nivel interno de la compañía, sin embargo las necesidades del negocio deben ser accedidas en un momento determinado desde las redes externas, es necesario implementar un procedimiento que establezca los requerimientos que deben ser tenidos en cuenta cuando la aplicación es trasladada del ambiente de producción LAN a el servidor DMZ. Por este motivo se genera un análisis de requerimiento para sistemas de información que involucre los aspectos que se debe tener en cuenta en la aplicación y en el *firewall*. Ya que el proceso de *hardening* de la DMZ se genera con otro proceso por eso no se involucra. Ver Cuadro 7.

Cuadro 7. Análisis de requerimientos para sistemas

1. Información general de proyecto	
Nombre del proyecto:	
Módulo o funcionalidad ***(nombre del módulo o funcionalidad si aplica)***	
2. Historia del documento	
Versión	
Que cambios se están proponiendo para el sistema de información o que nuevas funcionalidades se proponen	

Descripción de la situación actual
(Describir cómo funciona el sistema de información actual o como realizan en las actualidad las tareas los usuarios)

Lista de requerimientos funcionales (FR)
(Busque establecer respuestas a las siguientes preguntas)

Que procesos debe realizar el sistema de información, en caso de cambios describa los cambios, si es necesario anee diagramas de flujo del proceso o diagramas que ilustren las interacciones solicitadas.

Que entradas requiere el sistema de información para cada entrada; describa el tipo de dato, límites aceptables, criterios de validación y lista de datos que deben ser considerados como no validados

Dato	Limites	Criterios de validación	Valores considerados inválidos

Que salidas debe generar el sistema. Describa las salidas que se espera obtener:
Reportes
Actualización de tablas
Pantallas de resultados
Mensajes de comunicación con el usuario, otros procesos.
Conjunto de datos que se almacenaran como resultados

Que datos debe mantener el sistema.
Describa que información debe almacenar en forma permanente el sistema o la funcionalidad (tablas en bases de datos / archivos planos etc)

Con qué otros sistemas se relacionarán el sistema o la funcionalidad. Incluya un diagrama de relaciones de flujo de proceso que indique las interacciones a nivel de datos o control entre el sistema o la nueva funcionalidad con los sistemas actuales a nuevos sistemas que estén en desarrollo.

Cuadro 7. (Continuación)

Donde será almacenado el sistema. Indique en que servidores o repositorios de datos o bases de datos se almacenarán los datos del sistema o la nueva funcionalidad
Lista de requerimientos no funcionales (NFR) (Busque establecer respuestas a las siguientes preguntas)
¿Qué tiempos de respuesta se esperan para el sistema?
¿Qué volúmenes de datos se espera manejar?
¿Qué controles de seguridad se requieren para el sistema (contraseñas, cifrado de datos, validaciones, etc)?
¿Cuál es el volumen de usuarios que se espera atender?
¿Con qué perfiles de usuario debe contar el sistema?. Describa los roles de usuarios que se requieren para el sistema, indique en una tabla el rol y los permisos o funcionalidades que se asignaran a cada rol.
¿Qué tipos de acceso debe tener el sistema? Identifique si la funcionalidad será accesible vie WEB o mediante un cliente. Identifique si el servicio estará restringido a la red local o disponible desde ubicaciones externas.
¿Cuáles deben ser las restricciones de acceso al sistema? Identifique si hay horarios restringidos de acceso. Identifique si hay ubicaciones físicas desde donde no se debe tener acceso al sistema. Identifique si existen restricciones de fechas en las que no se debe tener acceso al sistema o la funcionalidad. Identifique si el usuario puede tener varias conexiones simultáneas al sistema.
¿Cuáles son los medios de salida del sistema? Identifique si las respuestas de la funcionalidad o del sistema se deben presentar por pantalla, por reporte o por mensajes de datos y que restricciones pueden tener esas salidas.
¿Cuáles deben ser los medios de almacenamiento aprobados para el sistema? Determine si los resultados se deben almacenar en disco duro, en medio impreso o en otros medios de almacenamiento como bases de datos remotas o servicios de almacenamiento externo.
¿Qué bases de datos manipula el sistema? Indique versión y modelo del motor de la base de datos, identifique nombre del servidor que contiene la bases de datos que usará o accederá el sistema o la funcionalidad.

Lista de requerimientos de facilidad de uso (Busque determinar qué tan “confortable debe ser el sistema para el usuario final”
¿Qué usuarios utilizaran el sistema? Describa perfiles o roles funcionales de los usuarios del sistema o la funcionalidad.
¿Qué tareas realizaran los usuarios? Describa las tareas que realizan los usuarios con la funcionalidad o el sistema.
¿Qué criterios de aceptación emplearan los usuarios para recibir el sistema? Describa el conjunto de pruebas que se realizaran para dar por aceptado el sistema/funcionalidad. Utilice el formato de casos de prueba para documentas las pruebas a ejecutar y aceptar el sistema/funcionalidad.

Cuadro 7. (Continuación)

¿Cuáles usuarios ejecutan las funciones privilegiadas en el sistema: usuarios administradores, usuarios auditores, usuarios de supervisión, etc?
¿Cuáles usuarios desempeñan funciones secundarias, como mantenimiento y administración?
Si el sistema interactúa con *hardware* externo o *software* describe el componente e incluya un diagrama de las interacciones de proceso o de flujo de datos del sistema con el componente.

Lista de requerimientos de seguridad de la información (Busque determinar que controles a nivel de seguridad de la información son necesario en el sistema
Se requiere cifrado de datos. Indique que datos se deben cifrar y que mecanismos se deben aplicar
¿Qué tipo de roles y perfiles a nivel de seguridad se necesitan: usuarios de auditoria, usuarios de supervisión?
¿Que controles de seguridad de información necesita el sistema/función? Determine si el sistema debe validar datos con fuentes externas, verifique si el ambiente de operación incluye condiciones hostiles (usuarios sin entrenamiento, usuarios potencialmente peligrosos para el sistema, usuarios no controlados por mecanismos de seguridad, usuarios con altos conocimientos en programación o seguridad informática)
¿Qué datos sensibles maneja en el sistema? Describa el dato y los controles de seguridad que se requieren.
Se requiere firma digital para la transmisión de información.
Se requiere almacenar información confidencial en medios removibles.
Describa otros requisitos de seguridad identificados durante el levantamiento de información.

Lista de requerimientos conexiones y *firewall*
¿Qué puertos se utiliza para generar consulta a la aplicación?
Describa que usuarios se conectaran a la aplicación
Horario en el cual va ser accedida la aplicación
IP publica relacionada al Dominio registrado
La aplicación ya cuenta con un certificado valido por una entidad certificadora y cumple con los parámetros de seguridad como TLS 1.2
Enumere las redes asociadas a la política de DMZ (se debe restringir el tráfico entrante y saliente solo a redes definidas)

Cuadro 7. (Continuación)

Modelamiento preliminar del sistema (De acuerdo con el modelo de desarrollo de *software*, anexe a continuación los diagramas que apliquen) Diseño estructurado: Diagrama de nivel 0 de flujo de datos del sistema, Diseño orientado a objetos: Diagrama de alto nivel de casos de uso Si emplea otros modelos de diseño, dibuje o describa el modelo preliminar del sistema
Espacio para el diagrama

Glosario de términos (Describa los términos que requieren una definición particular)	
Término	**Descripción**

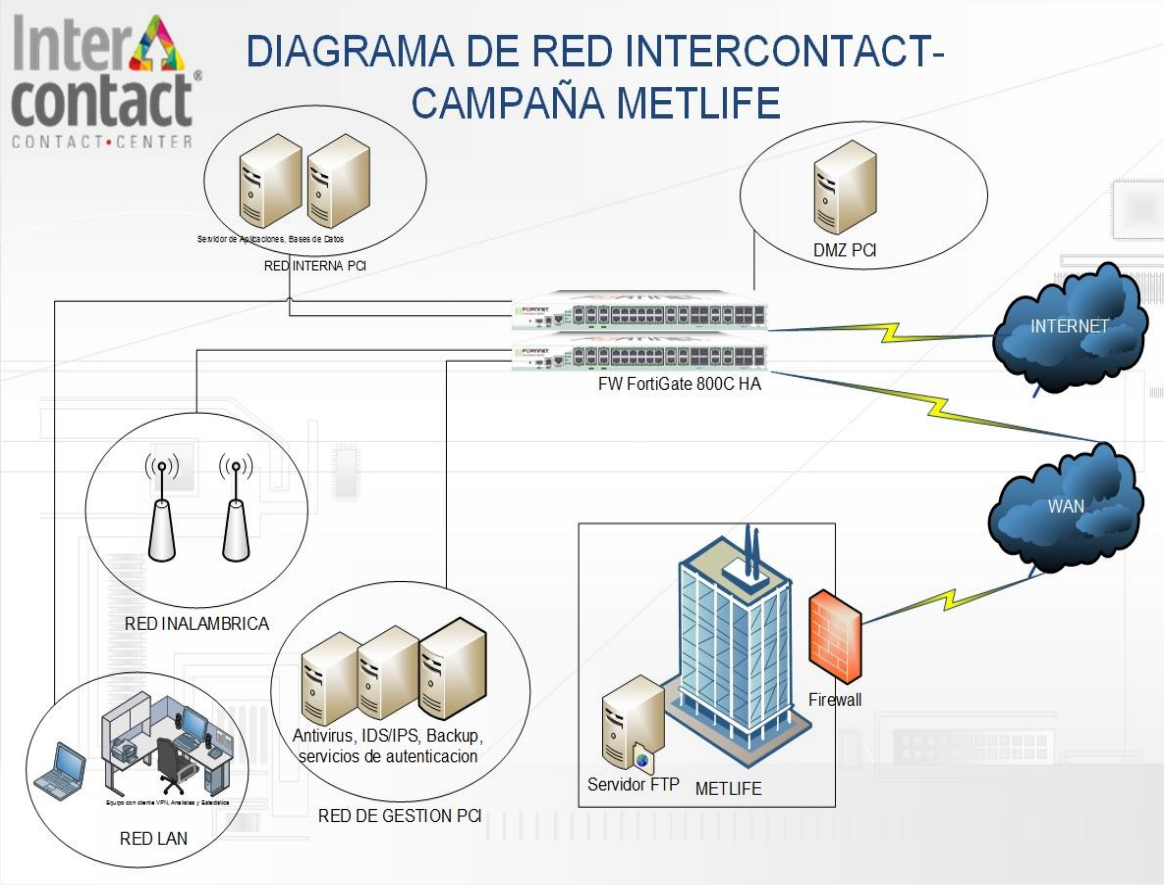
Recomendaciones (Si aplica, describa recomendaciones para el refinamiento de los requerimientos)	
Anexos (Si aplica, describa los anexos a este documento)	

Fuente: Elaboración propia, 2017

DIAGRAMAS

A continuación se muestra un diagrama ideal de red en PCI-DSS, el cual debe ser tenido en cuenta para ser configurado y restructurar la red en la cual todas las redes son aisladas mediante la interfaz del *firewall,* en esta puede generar una seguridad superior a los dispositivos de capa 3 que son usados actualmente para segmentar los diferentes entornos de los datos del titular de la tarjeta. Ver Figura 8.

Figura 8. Diagrama de red ideal PCI-DSS



Fuente: Elaboración propia, 2017

11.2 NO USAR LOS VALORES PREDETERMINADOS SUMINISTRADOS POR EL PROVEEDOR PARA LAS CONTRASEÑAS DEL SISTEMA Y OTROS PARÁMETROS DE SEGURIDAD

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 2 de la PCI DSS, se muestra a continuación. Ver Cuadro 8.

Cuadro 8. Configuración de sistemas para no usar valores predeterminados

Objetivo	Configurar los sistemas para no usar los valores predeterminados suministrados por el proveedor en relación a las contraseñas del sistema y otros parámetros de seguridad
Requerimientos cubiertos	2.1 – 2.6

Cuadro 8. (Continuación)

Acciones	▪ Los servidores de Telefonía y NAS debe tener una contraseña y usuario generadas por los administradores de plataforma de Intercontact. Solicitar al cliente que realice cambio periódico de contraseña en el FTP de manera periódica y que cumpla con requisitos mínimos para una contraseña segura. Deshabilitar o cambiar las contraseñas predeterminadas de los servidores NAS, de Telefonía, WSUS y los *Acces point*. Se debe involucrar aspectos como: Cambia valores y cuentas predeterminadas por el proveedor Deshabilitar todas las funcionabilidades innecesarias Implementar funciones seguridad adicionales para servicios que no se consideren seguros ▪ Documentar procedimiento sobre configuración de seguridad en los dispositivos de entornos inalámbricos (*Acces point*), servidores, *firewalls* y *switchs* que involucre cambio periódico de contraseña, sistema de cifrado, configuración de snmp, instalación, entre otros. Este procedimiento debe involucrar los parámetros de configuración, también del servidor radius y establecer la actualización del firmware. Y que no tenga configurado parámetros de cifrado débiles como WEP. Documentar los parámetros y valores específicos de seguridad que deben tener los servidores, equipos y dispositivos, junto con las funciones o servicios que deben estar habilitados de acuerdo al servidor. ▪ Estos procedimientos de configuración deben ser implementados antes de la salida a producción de un sistema o nueva plataforma. ▪ Verifique que se haya implementado una sola función principal por componente de sistema o dispositivo virtual. ▪ Implementar hardening en todos los servidores que tienen relación con la campaña metlife y estén involucrados con los datos del titular de la tarjeta. ▪ Configurar el servidor de aplicaciones y las aplicaciones relacionadas al uso de datos de titular de la tarjeta para que las aplicaciones antes de entrar a producción, funcionen por tls 1.2 o superior. Solicitar al cliente la configuración segura del FTP como FTPS o SFTP según lo que el cliente Metlife se le facilite y asegure en mejor medida su información.

Cuadro 8. (Continuación)

	▪ Deshabilitar el acceso por http de la consola de administración y aplicaciones de la campaña Metlife. ▪ Se debe involucrar en el inventario de activos existente todos los componentes relacionados con la campaña metlife y procesos que están involucrados en el tratamiento de los datos del titular de la tarjeta y actualizar este frecuentemente. ▪ Ampliar el detalle de informes de la plataforma *google*, con el fin de monitorear otros aspectos como son *drive, docs*, entre otros que ciertos perfiles tiene acceso.
Recursos	Recurso humano, capacitación en normas como la NIST
Tiempo	1 mes
Responsables	Administradores de plataformas tecnológicas, Director de tecnología, líder de mesa de ayuda.
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Los procedimientos de configuración de inalámbricos *Acces point*, servidores, *firewalls* y *switchs* deben estar alineados con normas de seguridad como ISO, CIS, NIST, SANST.
- El hardening de los diferentes servidores y sistemas se pueden basar en parámetros de auditorías de sistemas como las que se muestra en libros como IT *Auditing using controls to protect information assets* (Chris Davis and Mike Schiller).
- Generar configuraciones en el *firewalls* como A*ppplication Contol, Web Filters*, políticas anti DDoS, entre otros.
- Se debe generar documentación que establezca el uso de criptografía fuerte en la administración basada en Web basada en las mejores prácticas de la industria.
- Por ejemplo la extensión de clave un mínimo de 112 bits de solidez y algoritmos de cifrado AES (128 bits y superior), TDES/TDEA (claves de triple extensión), RSA (2048 bits y superior), ECC (224 bits y superior) y DSA/D-H (2048/224 bits y superior).

11.3 PROTEJA LOS DATOS DEL TITULAR DE LA TARJETA QUE FUERON ALMACENADOS.

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 3 de la PCI DSS, se muestra a continuación. Ver Cuadro 9.

Cuadro 9. Protección de datos que fueron almacenados

Objetivo	Proteger los datos del titular de la tarjeta que fueron almacenados en Intercontact
Requerimientos cubiertos	3.1 – 3.7
Acciones	▪ Establecer una reunión con el cliente Metlife para determinar y generar un procedimiento y políticas para la limitación de almacenamiento de datos del titular de la tarjeta y retención de los mismos de acuerdo a requisitos legales, reglamentarios y del negocio. ▪ Se debe establecer un proceso de eliminación segura de datos del titular de la tarjeta cuando estos ya no son necesarios por motivos legales, temas contractuales o reglamentarios basándose en el proceso de borrado seguro que existe actualmente en la compañía. Verificar que datos realmente son necesarios almacenar para el debido funcionamiento de la campaña Metlife. ▪ Establecer políticas que indiquen cuales son los únicos valores que deben ser almacenados en los cuales no puede ser involucrados el contenido completo de ninguna pista, el valor o código de validación de tarjetas, ni tampoco se puede solicitar ni almacenar el PIN ▪ Generar un documento que estipule las funciones o perfiles que están específicamente autorizadas para ver el número PAN completo. Enmascarar u ocultar los seis o los últimos cuatro dígitos del PAN, de modo que sea solo legibles para los perfiles específicos y definidos legalmente por una necesidad comercial. ▪ Convertir el número PAN en ilegible para su debido almacenamiento, utilizando técnicas como *hash*, truncamientos, *tokens* y criptografía sólida. ▪ Implementar un procedimiento donde se establezca un sistema para proteger el PAN utilizando algún sistema como *hash*, truncamiento, token o criptografía sólida. Todos los números PAN deben estar protegidos sin importar su lugar de almacenamiento. ▪ Cifrar las bases de datos que contienen datos del titular de

Cuadro 9. (Continuación)

	la tarjeta con un cifrado fuerte que cumpla con los del cliente, empresa y mejores prácticas de la industria. ▪ Establecer procedimientos y políticas para la protección de contraseñas que son usadas para la protección de datos del titular en todos sus ambientes (bases de datos, aplicaciones, cifrado de cd´s, almacenamiento de grabaciones, etc). ▪ Establecer protocolos de seguridad con el cliente Metlife para reforzar el acceso a la VPN y el FTP y custodiar las claves de acceso de acuerdo al procedimiento y políticas establecidas. Utilizar un protocolo seguro en vez de utilizar solo FTP, documentar que algoritmos de cifrado se están o se van a usar. ▪ Cifrar la información que debe ser cifrada de los datos del titular y las claves de cifrado de estas bases deben ser debidamente cifradas y restringidas al personal definido. ▪ Se deben crear un procedimiento para cifrar la información del titular de la tarjeta y administración de claves utilizadas para cifrar esta información. El método de envió de datos por medio del FTP debe involucrar métodos seguros para el envió de información con SFTP y SFTP, la clave de acceso de FTP debe terne un debido custodio, y esta debe ser cambiada con regularidad. Los parámetros de VPN utilizados deben generar también un cambio periódico de contraseña. Cuando se envié los datos de grabaciones cifradas en un CD la contraseña no solo puede estar en conocimiento a un solo funcionario de la compañía, el conocimiento debe ser compartido, las claves de cifrado deben ser seguras utilizando parámetros de seguridad como alfanuméricos, mayúscula, minúscula, números y mínimo 8 caracteres. ▪ Cuando se implemente el ciframiento de los datos del titular de la tarjeta se debe generar el procedimiento de generación de claves en el cual se debe involucrar aspectos que especifiquen la distribución de claves de manera segura en los cuales involucre aspectos como que solo se distribuyan a las personas específicas y nunca se haga en texto claro. Las claves de cifrado utilizadas se deben guardar de manera segura. ▪ Cuando se implemente el ciframiento de los datos del titular da la tarjeta, determinar un periodo de uso de claves para el uso de la misma durante un periodo definido. La gestión de claves el retiro o remplazo de claves cuando se presente

Cuadro 9. (Continuación)

	casos como retiro o remplazo de claves, remplazo de claves cuando se sospechen que están en riesgo y cuando un empleado es retirado de la compañía y conoce la clave. ▪ Involucrar en el procedimiento de gestión de claves aspectos que especifiquen actividades; prevenir la sustituciones de claves sin el debido permiso, también que se debe establecer la responsabilidad de los custodios donde aceptan y comprenden su responsabilidad como custodios de claves. ▪ Completar las políticas de seguridad de la información con aspectos detallados sobre la protección de datos del titular de la tarjeta y que esto sean de conocimiento a los funcionarios de la compañía.
Recursos	Capacitación en NIST, Recurso Humano, Herramienta de búsqueda de datos financieros, HSM, PTS, entre otros
Tiempo	4 meses
Responsables	DBA, Administrador de Servidores, Director de Tecnología
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Se recomienda guiarse de las buenas practicas dispuestas por la NIST para ejecutar un debido procedimiento de sanatización, para establecer una serie de criterios para la eliminación o destrucción segura de datos almacenados de forma intencional o no intencional para evitar que puedan ser restaurados como NIST *Special Publication* 800-88 - *Guidelines for Media Sanitization* - Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine -- Diciembre 2014.
- Para identificar que datos del titular de la tarjeta son almacenados se recomienda realizar una búsqueda automatizada con herramientas free como Cardito, CCSRCH, Find_SSNs, OpenDLP, Spider, entre otras.
- Se recomienda utilizar cualquiera de las siguientes técnicas que se nombran a continuación:
- Las funciones *hash* de una vía basadas en criptografía sólida se pueden utilizar para convertir los datos del titular de la tarjeta en ilegibles. Las funciones *hash* son apropiadas cuando no existe necesidad de recuperar el número original.
- El objetivo del truncamiento es eliminar permanentemente un segmento de los datos del PAN de modo que solo se almacene una parte (sin exceder los primeros seis y los últimos cuatro dígitos) del PAN.
- Un token de índice es un token criptográfico que reemplaza el PAN basándose en un índice determinado por un valor impredecible. Un ensamblador único es un sistema en el que una clave privada generada aleatoriamente solo se utiliza

una única vez para cifrar un mensaje, que luego se descifra utilizando un ensamblador y una clave únicos que coincidan.

- Cifrar la base de datos que están SQL con un cifrado seguro como AES 256, dado la base de datos SQL es superior a 2006, este se puede cifrar con ciertos parámetros de manera simétrica o asimétrica, para el entono de la compañía es recomendable simétrico. Las recomendaciones se pueden observar en el siguiente link https://msdn.microsoft.com/es-es/library/ms188357.aspx
- Cifrar las bases de datos que contiene la información de los datos del titular con un cifrado fuerte como AES256, la claves de cifrado deben ser debidamente custodiadas por un personal designado.
- Cuando se empiece a cifrar y a descifrar los datos del titular de la tarjeta, se debe utilizar técnicas para guardar estas claves con que se cifra o descifra con métodos como usar una clave de cifrado al menos tan sólida como la clave de cifrado de datos, utilizar un dispositivo criptográfico HSM, un dispositivo de punto de interacción aprobado para la PTS.
- Cuando se implemente el ciframiento de los datos del titular da la tarjeta se debe generar el procedimiento de generación de claves de cifrado que debe especificar como generar claves sólidas, de acuerdo a estándares como NIST *Special Publication* 800-133, ISO 11568-2 Servicios financieros, ISO 11568-4 Servicios financieros.

11.3.1 Políticas.

Política de eliminación y retención segura de datos en medio físico y lógico

ALCANCE

Esta política se aplica para cualquier dato del titular de la tarjeta manipulado por INTERCONTACT y que por necesidad de los servicios que presta a sus clientes, requiere ser procesada, almacenada y transferida, usando los sistemas de información o los servicios de tecnología de información de INTERCONTACT.

OBJETIVO

Garantizar la retención y eliminación segura y adecuada de los datos del titular de la tarjeta almacenados en medios físicos y lógicos en Intercontact, dando cumplimiento a requisitos legales, del cliente y mejores prácticas de la industria.

DETALLES

Condiciones obligatorias.

Los datos del titular de la tarjeta almacenados de forma intencional o no intencional

deben ser eliminados de manera segura para evitar que puedan ser restaurados, todo esto con base en su nivel de confidencialidad. Las técnicas de eliminación y/o destrucción segura deben garantizar la eliminación segura de la información y que esta no pueda ser recuperada bajo ninguna técnica. El cliente en conjunto con Intercontact debe definir las diferentes técnicas de eliminación de datos en medios lógicos que sean acordes con el negocio y de cumplimiento con cualquier regulación legal.

Los medios que contengan los datos de los titulares de la tarjeta deben ser destruidos cuando estos ya no sean necesarios para el negocio o por motivos legales.

Los controles para la eliminación o destrucción segura de datos deben ser acordes con las técnicas y métodos descritos en normas aceptadas por la industria, los métodos o técnicas a usar son las de Redactar, Borrado Seguro, Purgar y Destruir cuando el medio es físico.

El cliente debe definir ante Intercontact el tiempo adecuado de retención de los datos del titular que debe tener la compañía de acuerdo a su nivel de confidencialidad y cumplimientos legales. Intercontact a su vez debe identificar y eliminar de manera segura los datos almacenados que hayan excedido el periodo de retención estipulado.

RESPONSABILIDADES

Todos los empleados y contratistas de INTERCONTACT son responsables de cumplir la política de eliminación segura de datos.

Todos los empleados y contratistas de INTERCONTACT son responsables de reportar a la mayor brevedad la posible copia o hurto de datos del titular de la tarjeta que este almacenada o alojada en medios físicos y que está programada a ser eliminada y que se encuentren bajo su responsabilidad.

El área de informática debe mantener, coordinar y gestionar la eliminación segura de la información establecida en Intercontact.

Todo responsable del proceso que tenga empleados usando técnicas de eliminación segura de la información debe realizar seguimientos periódicos sobre el cumplimiento de la política de eliminación segura de datos en medios físicos y lógicos para certificar su cumplimiento.

SEGUIMIENTO Y CONTROL (MONITOREO)

La política de eliminación segura de la información de datos en medios físicos y lógicos debe ser revisada cada tres meses o cuando se presenten eventos que obliguen a su actualización.

Los responsables de tecnología, áreas y procesos realizarán seguimiento y control al cumplimiento de esta política.

Cumplimiento al numeral 3.1

Política de protección en el almacenamiento y visualización de datos

ALCANCE

Esta política se aplica para cualquier dato del titular de la tarjeta manipulado por INTERCONTACT y que por necesidad de los servicios que presta a sus clientes, requiere ser procesada, almacenada y transferida, usando los sistemas de información o los servicios de tecnología de información de INTERCONTACT.

OBJETIVO

Garantizar el almacenamiento seguro de datos de tarjetas de pago, prohibir el almacenamiento de datos confidenciales de autenticación y garantizar que sean ilegibles los datos del titular de la tarjeta que por cumplimiento de la PCIDSS deben permanecer así, dando cumplimiento a requisitos legales, del cliente y mejores prácticas de la industria.

DETALLES

Condiciones Obligatorias

En Intercontact está prohibido el almacenamiento del valor o código de validación de las tarjetas, el contenido completo de alguna pista y cualquier valor de autenticación después de recibir la autorización en cualquier medio de almacenamiento utilizado en Intercontact.

De igual manera está prohibido la solicitud del numero PIN al titular de la tarjeta y almacenar el mismo.

Se debe identificar las ubicaciones de almacenamiento inseguro de los datos del titular de la tarjeta que son almacenados en diferentes medios magnéticos, discos ópticos, cintas magnéticas, discos magneto-ópticos tarjetas de memorias, medios de almacenamiento removibles y realizar las acciones de aseguramiento de esta información aplicando controles que garanticen su confidencialidad, integridad y disponibilidad y corregir cualquier desviación. Para esta tarea se pueden emplear expresiones regulares o utilizar herramientas automatizadas específicas que faciliten la ejecución periódica de esta labor.

Enmascarar u ocultar los seis o los últimos cuatro dígitos del PAN de modo que sea

solo legibles para los perfiles específicos y definidos legalmente por una necesidad comercial.

El numero PAN debe permanecer ilegible en cualquier lugar donde este sea almacenado utilizando técnicas que garanticen la protección de los datos. Todos los números PAN deben estar protegidos sin importar su lugar de almacenamiento.

Las bases de datos que contienen datos del titular de la tarjeta deben estar cifradas con un algoritmo fuerte de cifrado de acuerdo a las mejores prácticas de la industria. Las claves de cifrado utilizadas deben ser debidamente custodiadas por el personal designado por la alta dirección o del proceso correspondiente.

RESPONSABILIDADES

Todos los empleados y contratistas de INTERCONTACT son responsables de cumplir la política de almacenamiento y visualización de datos.

Las claves de cifrado deben ser debidamente custodiadas únicamente por el personal designado por la alta dirección o por el dueño del proceso correspondiente.

Todos los empleados de INTERCONTACT son responsables de reportar a la mayor brevedad el posible almacenamiento no permitido de datos confidenciales, datos almacenados de manera visible y la copia o hurto de datos del titular de la tarjeta.

El área de informática debe mantener, coordinar y gestionar el almacenamiento seguro de la información, la prohibición de almacenamiento de datos establecidos en esta política y el enmascaramiento y ocultamiento del numero PAN.

Todo responsable del proceso que tenga empleados que soliciten datos del titular de la tarjeta confidenciales debe realizar seguimientos periódicos sobre el cumplimiento de la política de almacenamiento y visualización de datos para certificar su cumplimiento.

SEGUIMIENTO Y CONTROL (MONITOREO)

La política de almacenamiento y visualización de datos segura de la información debe ser revisada cada seis meses o cuando se presenten eventos que obliguen a su actualización.

Los responsables de tecnología, áreas y procesos realizarán seguimiento y control al cumplimiento de esta política.

Política de Claves

ALCANCE

Esta política se aplica a empleados, contratistas que prestan sus servicios a INTERCONTACT y a los empleados contratistas y terceros que tengan acceso a los recursos de información de la Entidad.

OBJETIVO

Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, usando claves fuertes y la protección de contraseñas usadas para la protección de datos.

DETALLE

Condiciones Obligatorias

La asignación de contraseñas se realiza de forma controlada mediante un procedimiento definido por el sistema de gestión de seguridad de la información. El área de tecnología es la única autorizada para la asignación de contraseñas para acceso a servicios, sistemas de información o equipos informáticos.

Los responsables de procesos, servicios o sistemas de información son los únicos autorizados para tramitar ante los administradores de sistemas de información o equipos de tecnología la asignación de cuenta de usuario y contraseña para los empleados, contratistas y terceros que presten sus servicios a INTERCONTACT.

Cualquier servicio, sistema de información o equipo informático que tenga contraseñas por defecto configuradas por el proveedor o fabricante deben ser cambiadas por nuevas contraseñas cuando se realice el proceso de configuración del servicio, sistema o equipo. Al momento de poner en producción el servicio, sistema o equipo se debe volver a cambiar la contraseña por una nueva.

La contraseña asignada a un usuario es personal e intransferible. Los usuarios no deben divulgar, prestar, exhibir, comunicar en forma escrita o verbal su contraseña. Cuando por labores de soporte o mantenimiento se requiere la contraseña de usuario, el usuario es quién debe digitarla y al final de las actividades de soporte se debe cambiar por una contraseña nueva.

Los usuarios deben cambiar por lo menos cada mes sus contraseñas de acceso a servicios, sistemas de información o equipos informáticos.

Los administradores de servicios, sistemas de información, equipos informáticos deben cambiar sus contraseñas una (1) vez al mes.

Los administradores de servicios, sistemas de información, equipos informáticos deben utilizar contraseñas diferentes para sus cuentas de usuario y para sus cuentas como administradores.

Las claves usadas para la protección de datos del titular de tarjeta deben tener asignados custodios específicos asignados por los dueños del proceso o la alta dirección, estos se deben limitar al menor número posible de custodios.

Los usuarios son responsables de todas las acciones que se realicen con sus contraseñas. En caso de que la contraseña haya sido conocida por terceros, el usuario debe informar inmediatamente al responsable del proceso o del área y al área de tecnología para bloquear cualquier acceso a servicio, sistema de información o equipo informático que utilizará la contraseña comprometida.

Las contraseñas almacenadas en los servicios, sistemas de información y equipos informáticos de INTERCONTACT, deben estar almacenadas en formato cifrado cumpliendo con la política de controles criptográficos de INTERCONTACT y las mejores prácticas actuales de la industria.

Las claves de cifrado usadas para cifrar claves deben ser al menos tan sólidas como las claves usadas para almacenar los datos, estas claves de cifrado de claves deben ser almacenadas de manera separada que las claves de cifrado de datos.

El almacenamiento de contraseñas debe destinar la menor cantidad ubicaciones y formas posibles

Usos no autorizados

El uso de *software* para visualizar, descifrar o interceptar contraseñas de servicios, sistemas de información o equipos informáticos de INTERCONTACT está prohibido.

Utilizar la contraseña para otros fines que no estén establecidos.

RESPONSABILIDADES

Cada usuario debe tener en cuenta las buenas prácticas de seguridad de selección y uso de sus contraseñas que defina el sistema de gestión de seguridad de la información de INTERCONTACT.

- Responsabilidades de los usuarios

Cambiar SIEMPRE en forma inmediata la contraseña que le asignen en el primer acceso a los servicios, sistemas de información o equipos informáticos.

Mantener la contraseña en estricto secreto, nunca por ninguna circunstancia se debe divulgar a nadie.

El número de custodios de claves de encriptación debe estar debidamente identificado y designado por la alta dirección o por los dueños del proceso con aprobación de la alta dirección.

Cambiar periódicamente la contraseña de usuario, al menos una vez cada tres (3) meses y si se tiene rol de administrador al menos una (1) vez al mes.

Cambiar mínimo una (1) vez cada mes las contraseñas de administración de servicios, sistemas de información o equipos informáticos.

Cambiar periódicamente las claves criptográficas al menos una vez cada tres meses o de acuerdo con las mejores prácticas de la industria.

Se debe retirar o remplazar las claves cuando se presente casos como retiro o remplazo de claves, remplazo de claves cuando se sospechen que están en riesgo y cuando un empleado es retirado de la compañía y conoce la clave.

No usar las contraseñas asignadas por INTERCONTACT en servicios que no son de INTERCONTACT, ejemplo servicios gratuitos de correo electrónico, mensajería instantánea o redes sociales y viceversa no usar las contraseñas de servicios gratuitos en los servicios, sistemas de información y equipos informáticos de INTERCONTACT.

- Responsabilidades del área de Tecnología

Además de las obligaciones descritas en la política de gestión de claves, los administradores de servicios, sistemas de información y equipos informáticos deben:

Aplicar el procedimiento de creación de cuentas y contraseñas definido por el sistema de gestión de seguridad de la información de INTERCONTACT.

Realizar verificación periódica de contraseñas débiles e informar al responsable del servicio, sistema de información o equipo para que aplique medidas correctivas.

Cuando se detecte que una contraseña ha sido comprometida, debe seguir el procedimiento de gestión de incidentes de seguridad, mitigar el impacto del incidente cambiando las contraseñas de los sistemas identificados como comprometidos y evaluar la extensión del incidente para determinar el cambio de contraseñas en otros sistemas no comprometidos.

SEGUIMIENTO Y CONTROL (MONITOREO)

La política de claves debe ser revisada cada seis meses o cuando se presenten eventos que obliguen a su actualización.

Política de controles criptográficos y llaves criptográficas

ALCANCE

Esta política aplica para cualquier información que sea gestionada, almacenada, trasmitida o transportada usando la infraestructura de tecnología de información y comunicaciones, o medios de almacenamiento de INTERCONTACT y que de acuerdo con su nivel de clasificación o riesgos a los que puede estar expuesta debe ser cifrada para evitar su acceso a personas o sistemas de información no autorizados.

OBJETIVO

Definir la gestión de controles criptográficos para el envío o recepción de información en medios electrónicos protegiendo la confidencialidad, integridad y trazabilidad de la información.

DETALLE

Condiciones Obligatorias

La información de carácter confidencial o que por los procesos en que se utilice esté expuesta a riesgos de pérdida de confidencialidad se debe cifrar.

El Sistema de Gestión de Seguridad de la Información de INTERCONTACT determinará los mecanismos de cifrado de datos que mejor se ajusten a las necesidades específicas de cada tipo de información.

Las contraseñas para cifrado de información se deben proteger y gestionar siguiendo los controles de seguridad definidos para la protección de contraseñas de INTERCONTACT

Para el cifrado de información se utilizaran algoritmos de cifrado asimétricos.

Los computadores portátiles, medios de almacenamiento removibles y medios de respaldo que contengan información clasificada con carácter confidencial deben ser sometidos a cifrado de datos.

Cuando se utilicen sistemas de intercambio de información como correos electrónicos, sistemas de transferencias de datos o sistemas de información para intercambio de datos con otras entidades en los que viaje información con carácter confidencial deben emplear mecanismos de cifrado autorizados por los responsables de áreas y procesos de INTERCONTACT.

Al realizar el cifrado de información, se debe mantener copia de las llaves de cifrado en lugar seguro de forma que la recuperación de la información cifrada sea factible

en caso de ausencia temporal o permanente del custodio de la información cifrada.

Toda llave de cifrado utilizada en entornos de pruebas y desarrollo no deben ser instaladas en producción.

Se deben generan claves criptográficas sólidas (AES-256), garantizar que su distribución es independiente a la distribución de la información cifrada.

Definir el almacenamiento de las claves en dispositivos seguros y realizar cambios periódicos de las claves.

Las llaves criptográficas de las que se tenga sospecha de exposición deben ser destruidas, así como definir tiempos de vida de las claves.

El proceso de creación de llaves criptográficas y su conocimiento y control deben estar bajo la responsabilidad de diferentes personas, así como hacer firmar a estos custodios un formato donde se garantice que comprenden y aceptan su responsabilidad frente a las llaves criptográficas.

Usos no autorizados

Está expresamente prohibido cifrar información con mecanismos no autorizados por el Sistema de Gestión de Seguridad de la Información de INTERCONTACT

Está expresamente prohibido cifrar información sin la autorización del custodio de la información.

Está expresamente prohibido revelar las claves privadas de cifrado de información a personal no autorizado.

RESPONSABILIDADES

Los responsables de información, procesos, procedimientos o actividades que impliquen procesamiento, transmisión o almacenamiento de información empleando medios electrónicos deben solicitar mediante los procedimientos definidos por INTERCONTACT, el cifrado de la información clasificada como CONFIDENCIAL que esté bajo su responsabilidad.

El área de tecnología de INTERCONTACT es la responsable de documentar, divulgar y actualizar los procedimientos para el cifrado de información incluidas las actividades de generación, gestión y protección de las claves empleadas para el cifrado de información.

SEGUIMIENTO Y CONTROL (MONITOREO)

La política de controles criptográficos debe ser revisada cada seis meses o cuando

se presenten eventos que obliguen a su actualización.

11.4 CIFRAR LA TRANSMISIÓN DE LOS DATOS DEL TITULAR DE LA TARJETA EN LAS REDES PÚBLICAS ABIERTAS

El plan de acción que se llevara a cabo para dar cumplimiento al requisito 4 de la PCI DSS, ses muestra a continuación. Ver Cuadro 10.

Cuadro 10. Ciframiento de la transmisión de los datos de la tarjeta en las redes públicas abiertas

Objetivo	Cifrar la transmisión de los datos del titular de la tarjeta en redes públicas abiertas
Requerimientos cubiertos	4.1 -4.3
Acciones	▪ El servidor FTP que se tiene para alojar y descargar información del titular de la tarjeta debe tener una configuración de seguridad adecuada, debe utilizar un protocolo seguro, además de crear perfiles concretos para cada usuario y cambio periódico de contraseña. Se debe establecer en conjunto con el cliente un servicio en FTPS o SFTP según sea lo más conveniente y fácil para el cliente. ▪ Documentar políticas y procedimientos que establezca la configuración segura para el transporte seguro de información con claves, certificados de confianza, que solo se acepte versiones y configuraciones seguras y cifrado sólido. ▪ Configurar la aplicación Web que se usa a nivel LAN con https y habilitar TLS 1.2 o superior al trasmitir o recibir los datos del titular de la tarjeta. ▪ Genere la debida documentación y procedimientos para el debido acceso y configuración de un equipo a la red inalámbrica como se conecta los visitantes y los funcionarios de la compañía, de igual manera establecer documentalmente el tipo de protocolo y mejores prácticas de seguridad de la industria que deben tener configurados los *Acces point*. Configurar para que los *access point* solo puedan ser accedido de manera segura por protocolos como https. ▪ Cifrar el numero PAN en las transmisiones de este por el

Cuadro 10. (Continuación)

	FTP o el aplicativo web, se debe establecer políticas que establezcan que los PAN no protegidos no se deben enviar por medio de tecnología de usuario final. ▪ Se debe implementar procedimientos y políticas que establezcan que los datos del titular de la tarjeta sean cifrados en las transmisiones y que estos sean documentados, estén en uso y sean de conocimiento para todas las partes interesadas.
Recursos	Herramientas de validación si los aplicativos son vulnerables SSL/TLS. Recurso Humano, herramientas de cifrado.
Tiempo	1 Mes y Medio
Responsables	Recurso Técnico de Intercontact y de Metlife, Director de Tecnología, Líder del sistema integrado de gestión, Ingeniero de Infraestructura, DBA
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Ninguno de los datos del titular de la tarjeta están públicos en páginas web publicas solo en páginas a nivel LAN y en la aplicación FTP de Metlife, sin embargo es bueno aplicar las mejores prácticas para mitigar las vulnerabilidades expuestas a nivel SSL/TLS inferiores a 1.2 como se exponen en el siguiente sitio https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
- Identificar que las siguientes vulnerabilidades no estén presentes en las aplicaciones que manejen datos del titular de la tarjeta:

  BEAST **(“***Browser Exploit Against* SSL/TLS”) – CVE-2011-3389
  CRIME (“C*ompression Ratio Info-leak Made Easy*”) – CVE-2012-4929
  BREACH (“B*rowser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext*”)
  HEARTBLEED – CVE-2014-0160
  POODLE (“*Padding Oracle On Downgraded Legacy Encryption*”) – CVE-2014-3566
  FREAK (“*Factoring Attack on RSA-EXPORT Keys*”) – CVE-2015-0204
  logjam – CVE-2015-4000
- Emplee algoritmos robustos en las configuraciones de cifrado de SSL/TLS (evitar el uso de Triple-DES CBC, RC4, MD5 y SHA-1)
- Se pueden usar ciertos comandos con nmap para identificar si el sitio web es vulnerable por ejemplo a *Heartbleed*

  nmap –p 443 –script ssl –heartbleed (HOST)
  Para verificar que algoritmos de cifrado permitidos en el sitio Web que

maneja los datos del titular de la tarjeta.
nmap --script ssl –enum-ciphers –p 443 (HOST)

11.5 PROTEGER LOS SISTEMAS CONTRA MALWARE Y ACTUALIZAR LOS PROGRAMAS O *SOFTWARE* ANTIVIRUS REGULARMENTE

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 5 de la PCI DSS, se muestra a continuación. Ver Cuadro 11.

Cuadro 11. Protección de los sistemas contra malware

Objetivo	Proteger los sistemas contra malware y actualizar los programas el antivirus regularmente
Requerimientos cubiertos	5.1 – 5.4
Acciones	▪ Evaluar el desempeño que la consola de antivirus ejerce sobre los equipos y servidores. ▪ Aunque los servidores de telefonía tienen acceso limitado a internet, se debe evaluar que estos sistemas no se vean afectados por ningún tipo de malware. ▪ Definir la periodicidad para la ejecución de análisis del antivirus en los equipos y servidores de la compañía. Verificar que este configurado en la consola de antivirus la ejecución de análisis periódicos y documentar la frecuencia del mismo en la política de antivirus. ▪ Se debe conservar los registros de auditoria de la consola de antivirus con el fin de proporcionar la supervisión del antivirus. ▪ Definir procedimientos documentados que establezcan las actividades que se deben llevar a cabo cuando es necesario desactivar la protección del antivirus, por ejemplo deshabilitar el acceso a internet y realizar un análisis completo cuando este se vuelva a habilitar.
Recursos	Asesoría externa (proveedor de Antivirus), recurso técnico
Tiempo	15 días
Responsables	Administrador de consola de antivirus, Director de tecnología
Fuente: Elaboración propia, 2017	

11.6 DESARROLLAR Y MANTENER SISTEMAS Y APLICACIONES SEGURAS

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 6 de la PCI DSS, se muestra a continuación. Ver Cuadro 12.

Cuadro 12. Desarrollo y mantenimiento seguro de las aplicaciones y sistemas

Objetivo	Desarrollar y mantener los sistemas y aplicaciones seguras
Requerimientos cubiertos	6.1 – 6.7
Acciones	▪ Dado que el análisis de vulnerabilidades que se realiza es a nivel interno, se requiere se revisen ciertos criterios para la evaluación de las vulnerabilidades y asignar la clasificación de riesgo a esas vulnerabilidades basándose en un proceso que controle activamente las fuentes de la industria para obtener información sobre las vulnerabilidades. ▪ Involucrar en las políticas de Intercontact la instalación de parches que deben ser aplicados tanto en estaciones de trabajo como en servidores, tiempos máximos para la instalación y deben estar actualizadas con relación al mes de su publicación. Por ejemplo los parches críticos deben ser instalados mensualmente. ▪ Involucrar formalmente la seguridad de la información durante todo el ciclo de vida del *software* en los requisitos, el diseño, el análisis y las fases de prueba de desarrollo, por ejemplo estableciéndolo en el flujo grama del proceso, o la política de desarrollo estos aspectos. ▪ Documentar a nivel procedimental en el proceso de desarrollo de aplicaciones la eliminación de los ID de usuarios y contraseñas utilizadas en los ambientes de prueba antes que estas salgan a producción. ▪ Todos las aplicaciones que van a salir a producción deben ser aprobadas por el comité de cambios o en su defecto por la gerencia, de igual manera las pruebas de seguridad deben ser realizadas antes de su salida a producción. Se debe asignar una persona distinta al desarrollador para realizar las revisiones de código y pruebas cuando se generen cambios en estos, esta persona debe tener conocimientos en técnicas de revisión de código. ▪ El funcionario encargado para realizar el proceso de desarrollo y pruebas, debe ser distinto del que configura la aplicación al ambiente de producción.

Cuadro 12. (Continuación)

	▪ El desarrollador solo debe tener acceso a los ambientes de desarrollo y pruebas, la aplicación debe ser aplicada a producción por un funcionario distinto. Se debe bloquear el acceso al desarrollador al ambiente de producción. Se debe designar, y asignar funciones a un cargo del proceso de tecnología que involucren la configuración de las aplicaciones que van a salir a producción. ▪ Incluir en el procedimiento de desarrollo el paso en el cual se indique que los datos que están en producción no pueden ser utilizados en los ambientes de pruebas ni desarrollo. ▪ Complementar el procedimiento de gestión de cambios con aspectos como la documentación de la incidencia, aprobación del cambio por las partes autorizadas, pruebas de funcionabilidad, procedimientos de desinstalación, documentación de la incidencia que genero el cambio o actualización en la aplicación y el impacto del cambio. ▪ Documentar los cambios que son autorizados por el cliente a nivel de aplicaciones. ▪ Verificar que el entorno a nivel de seguridad no se reduce al implementar el cambio y que los controles de seguridad antiguamente instalados no hayan desmejorado en su efectividad o se remplacen por controles igualmente sólidos. ▪ Documentar un procedimiento de desinstalación cada vez que se realiza un cambio en una aplicación, para permitir devolver cambios en caso que el cambio falle o la seguridad en el sistema aplicación sea afectada. ▪ Asegurarse que por lo menos anualmente se capacite al personal desarrollador de la compañía en técnicas seguras de codificación, incluida la forma de evitar las vulnerabilidades más comunes. ▪ Incluir en el procedimiento de desarrollo los siguientes aspectos: Técnicas de codificación que aborden los errores de inyección Técnicas de codificación que aborden los desbordamientos de buffer, con aspectos como validación de límites de buffer y truncamiento de cadenas de entrada. Técnicas de codificación que autentiquen y cifren correctamente todas las comunicaciones

Cuadro 12. (Continuación)

	confidenciales. Manejo adecuado de errores, para evitar exponer información privilegiada mediante métodos de manejo de errores. Validación de todos los parámetros antes de la inclusión y uso de técnicas de escape sensibles al contexto (XSS). Manejo de referencia directa insegura a objetos, que incluya aspectos como autenticación correcta de usuarios, desinfección de entradas, no exposición de referencias a objetos internos a usuarios. Actividades para la corrección de CSRF (falsificación de solicitudes entre distintos sitios) Actividades como tokens de sesión, no exposición de los ID de la sesión en la URL y la incorporación de tiempos de espera apropiados y rotación de las ID de la sesión después de iniciar sesión satisfactoriamente. ▪ Los indicadores relacionados con la solución de vulnerabilidades deben estar directamente relacionados con los indicadores que rigen al proceso de desarrollo, las vulnerabilidades en alta detectadas, deben ser solucionadas y aplicadas en las aplicaciones en producción y corregidos en las que están en el proceso de desarrollo. ▪ Realizar validaciones de seguridad cuando las aplicaciones que son accedidas a nivel LAN deben ser accedidas en un momento determinado desde el servidor DMZ. ▪ Involucrar un análisis de seguridad de vulnerabilidades de las aplicaciones por lo menos una vez al año.
Recursos	Capacitación en técnicas seguras de codificación, recurso humano, asesoría externas, equipos o servidores para la implementación de procedimientos.
Tiempo	1 Meses y Medio
Responsables	Equipo de Desarrollo, DBA, Personal de Tecnología, Directores de desarrollo y Tecnología
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Verificar que las herramientas que se utilicen para realizar análisis de vulnerabilidades clasifiquen sus vulnerabilidades basando su riesgo de factor en CVSS.

- Si se va a realizar un análisis de vulnerabilidades se recomienda que se use un proveedor aprobado de escaneo cuyos criterios de valoración de vulnerabilidades de manera correcta a continuación se muestra el siguiente enlace que ayuda a verificar los proveedores aprobados por la industria. https://es.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
- Revisar el proceso de desarrollo, para involucrar actividades de desarrollo seguro como el libro de la OWASP - *A Guide to Building Secure Web Applications and Web Services* - 2.0 Black *Hat Edition*, también el libro *Software Security Building Security in Gary McGraw - Addison-Wesley*
- El procedimiento de desinstalación puede estar asociado al procedimiento de gestión de cambios incluyendo o usando criterios que este utiliza.
- Los desarrollos en la compañía deben basar en estas normas de codificación segura, estas normas de codificación segura pueden ser la guía de la OWASP, estándares de codificación segura CERT, entre otros.
- Se puede usar cifrado simétrico a nivel LAN en el uso de aplicaciones con algoritmos como AES256.
- Se sugiere tener *logs* de auditoria que aplique en la política relacionada a la DMZ, implementar en la política del *firewalls* parámetros de IPS además de implementar un equipo WAF por ejemplo un M*odSecurity.*

11.7 RESTRINGIR EL ACCESO A LOS DATOS DEL TITULAR DE LA TARJETA SEGÚN LA NECESIDAD DE SABER QUE TENGA LA EMPRESA

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 7 de la PCI DSS, se muestra a continuación. Ver Cuadro 13.

Cuadro 13. Restricciones al acceso de los datos del titular de la tarjeta

Objetivo	Restringir el acceso a los datos del titular de la tarjeta de acuerdo a las necesidades entre Intercontact y Metlife
Requerimientos cubiertos	7.1 – 7.3
Acciones	▪ Definir, establecer y documentar parámetros más restrictivos a la información que accede los funcionarios de la compañía dependiendo de cada cargo, función y clasificación de la información con el fin de limitar el acceso a los datos de los titulares de la tarjeta y diferentes componentes del sistema. Asegurarse que ningún funcionario podrá tener acceso a los datos del titular de la tarjeta a menos que esté definido dentro de sus funciones. Estos accesos privilegiados deben cumplir parámetros específicos en su asignación y así sean otorgados a la

Cuadro 13. (Continuación)

	menor cantidad posible de funcionarios. ▪ Definir por cargo o perfil los componentes del sistema a los cuales debe tener acceso con el fin de que ejerza su labor y el nivel de privilegio. ▪ Complementar el procedimiento de asignación de roles y privilegios, para determinar el debido procedimiento para asignar el nivel de acceso o privilegios que va a tener el funcionario, de igual manera vincular en el perfil del funcionario los privilegios a los cuales este puede acceder de acuerdo al cargo. No se pueden asignar privilegios sin pasar por un debido procedimiento de aprobación. ▪ Reforzar el procedimiento de creación, modificación y eliminación de usuarios en los que se relacione el cargo con el debido perfil para poder limitar con mayor cuidado el acceso a componentes del sistema, información, privilegios, accesos, entre otros. ▪ Documentar en procedimientos, políticas y llevar el debido seguimiento para que el control de acceso se implemente en todos los componentes del sistema. ▪ Cuando se actualicen y documente los diferentes políticas y procedimientos de control de acceso y métodos para otorgar privilegios estos deben ser informados y publicados a todas las partes interesadas.
Recursos	Recurso Humano
Tiempo	15 días
Responsables	Administradores de las plataformas tecnológicas, Director de tecnología, DBA, Desarrollador, Director de Operaciones.
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Proteger los datos más importantes, estén donde estén, analizar automáticamente toda la actividad del entorno de datos con el objetivo de minimizar riesgos, proteger datos sensibles frente a amenazas internas y externas y adaptarse a los cambios que afectan a la seguridad de los datos de forma transparente por ejemplo con un *IBM Security Guardium Data Protection for Databases*
- Implementar un sistema de centralizado de control de acceso para que otorgue de manera unificada el acceso y privilegios tanto a información y a sistemas de manera controlada.

11.8 IDENTIFICAR Y AUTENTICAR EL ACCESO A LOS COMPONENTES DEL SISTEMA

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 8 de la PCI DSS, se muestra a continuación. Ver Cuadro 14.

Cuadro14. Identificación y autenticación del acceso a los componentes del sistema

Objetivo	Identificar y autenticar el acceso a todos los componentes del sistema.
Requerimientos cubiertos	8.1 – 8.8
Acciones	▪ Generar un seguimiento más juicioso a los *logs* de logueo de usuarios para evidenciar ciertos eventos o incidencias. ▪ Solicitar al cliente Metlife la creación de perfiles con respectivo ID y usuario para identificar y determinar cada rol y usuario y a qué nivel de privilegios puede acceder. ▪ En varias ocasiones en el cambio de cargo no se realiza la solicitada de modificación de perfiles o acceso a todas la plataformas, estas pueden incluir el acceso a la los datos del titular de tarjeta, formalizar de manera adecuada este procedimiento. ▪ Realizar la eliminación o deshabilitación de usuarios de todas las plataformas y sistemas, incluido los sistemas de acceso físico lo más rápido posible. El procedimiento de paz y salvo debe ser más efectivo con el fin que el funcionario este a paz a salvo antes de abandonar la compañía. ▪ Realizar el debido monitoreo de los proveedores o terceros mientras acceden a los sistemas de Intercontact y deshabilitar los accesos mientras estos no se usen. Establecer horarios de acceso con el fin que solo se use cuando en el horario establecido y se deshabiliten automáticamente. Además se debe definir el nivel de acceso que tienen estos a la información y a los sistemas. ▪ El procedimiento de gestión de usuarios y contraseñas debe regir en todos los sistemas que involucran los datos del titular de la tarjeta como son el aplicativo de la planta telefónica (acceso a grabaciones), FTP proporcionado por el cliente y todas las aplicaciones. ▪ Actualizar las políticas o procedimientos que involucren los siguientes aspectos: ▪ Indicar que el máximo tiempo que una sesión este inactiva

Cuadro 14. (Continuación)

	antes de que vuelva a solicitar de nuevo ingreso de usuario y contraseña es 15 minutos, esto debe aplicar para todos los sistemas (directorio activo, planta telefónica, aplicaciones, entre otros). Solicitar a Metlife esta configuración de sesión inactiva en el servicio FTP y VPN. Las contraseñas deben estar ilegibles durante su trasmisión y almacenamiento en los sistemas utilizados por Intercontact, también documentar el debido procedimiento de desbloqueo o restablecimiento de contraseña con el fin de garantizar que realmente la persona que solicita el desbloqueo o restablecimiento de la contraseña sea la correcta o al propietario de la misma. El bloqueo de las cuentas de usuario cuando se bloqueen permanezcan mínimo 30 minutos bloqueadas o que su desbloqueo se realice directamente por el administrador del sistema. Se debe ampliar el bloqueo de sesión por errores continuos en el ingreso de contraseña mínimo a 30 minutos involucrar la plataforma de telefonía en esta configuración. Solicitar al cliente Metlife que realice este tipo de configuraciones en las plataformas usadas en Intercontact. El máximo ingreso de ID y contraseña erróneo a los diferentes sistemas de Intercontact no debe superar 6 intentos. Se debe involucrar en todos los sistemas en los cuales el usuario final tiene acceso incluyendo la plataforma de telefonía. Solicitar al cliente Metlife que el aplicativo FTP bloquee el usuario cuando este ingrese la contraseña erróneamente 6 veces. Las cuentas de usuario desactivadas en el directorio activo se eliminen máximo cada 90 días, también establecer que todas las cuentas de usuario de las demás plataformas también sean eliminadas máximo cada 90 días. Establecer que los sistemas soliciten al usuario la renovación de su contraseña mínimo cada 90 días, se deben involucrar todos los sistemas que están relacionados con los datos del titular de la tarjeta como son los aplicativos de la planta telefónica (mitrol) y los aplicativos proporcionados por el cliente Metlife (VPN, FTP). Todos los sistemas que involucren los datos del titular de la tarjeta el bloqueo de uso repetido de contraseña por lo menos las últimas cuatro contraseñas, solicitar que esto

Cuadro 14. (Continuación)

	también se realice en los aplicativos proporcionados por el cliente Metlife. Establecer el cambio de contraseña en el primer ingreso al sistema en el caso de las estaciones de trabajo, aplicaciones, Mitrol, entre otros. ▪ Implementar un sistema de autenticación de doble factor a nivel de acceso administrativo individual que no sea de consola y todo acceso remoto al entorno de los datos del titular de la tarjeta, el acceso a la bases de datos y a la grabaciones que contiene datos del titular de la tarjeta. ▪ Involucrar autenticación de doble factor al menos en el acceso remoto por los administradores del sistema y proveedores que podrían tener acceso a los datos del titular de la tarjeta por ejemplo el proveedor de telefonía Mitrol. ▪ Deshabilitar el usuario administrativo utilizado para realizar configuraciones en las estaciones de trabajo o servidores, cada funcionario de soporte debe utilizar un usuario individual con ciertos niveles o privilegios para realizar las debidas configuraciones que son requeridas para ejecutar sus labores. ▪ Identificar que otros sistemas deben reforzar el sistema de autenticación, e involucrar sistemas de autenticación dobles o triples, por ejemplo servidores de bases de datos o donde se alojan las grabaciones. ▪ Realizar configuraciones para que solo el administrador de la base de datos sea el único que puede acceder directamente a la base de datos para realizar consultas. Los métodos de acceso, consulta, mover, copiar y eliminar en la base de datos se deben realizar únicamente mediante métodos programáticos, por ejemplo a través de procedimientos almacenados y no, a través del acceso directo a la base de datos por parte de usuarios finales.
Recursos	Recurso Humano, Adquisición de soluciones que faciliten la configuración de sistemas por ejemplo la autenticación de doble factor.
Tiempo	2 Meses
Responsables	Director de tecnología, Administradores de plataformas, Desarrollador, DBA, Director de operaciones y Líder integrado del sistema de gestión,
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Esta información debe ser ilegible mediante el uso de una criptografía sólida como AES256 o con el uso de un *hash* como SHA1 o superior. Se debe involucrar en esto los sistemas como el directorio activo, los *Acces point*, las aplicaciones, bases de datos, servidor planta telefónica, entre otros.
- La autenticación de múltiples factores puede realizarse, ya sea tras la autenticación para la red en particular o para el componente del sistema. Por ejemplo en el acceso a la base de datos donde esta los datos del titular de la tarjeta.
- La autenticación doble factor se puede emplear por ejemplo el envió de un correo electrónico con un clave a parte de la clave ya usada para ingresar al sistema, se puede también implementar *tokens*, o la recepción de un sms con un código para poder ingresar, a parte del uso de la contraseña.
- Completar el procedimiento de gestión de usuarios, contraseñas, perfiles indicando las buenas prácticas para proteger las credenciales de autenticación no escribir las contraseñas ni guardarlas en archivos no seguros y estar atentos a personas malintencionadas que intenten hurtar sus contraseñas (por ejemplo, llamar a un empleado y solicitar su contraseña para poder "solucionar el problema"), el prohibido uso de contraseñas usadas con anterioridad, configuración de esto en los diferentes sistemas para que no permita usar por lo menos las últimas 4 contraseñas usadas.
  Los pasos a seguro para cambiar las contraseñas en los sistemas si se sospecha que esta contraseña está corriendo riesgos. También completar en el procedimiento una pequeño instructivo de cómo elegir una contraseña segura, por ejemplo el no uso de palabras de diccionario, datos de la persona como nombres de familiares, fechas, entre otros.

11.9 RESTRINGIR EL ACCESO FÍSICO A LOS DATOS DEL TITULAR DE LA TARJETA

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 9 de la PCI DSS, se muestra a continuación. Ver Cuadro 15.

Cuadro15. Restricción al acceso físico a los datos del titular

Objetivo	Restringir el acceso físico a los datos del titular de la tarjeta
Requerimientos cubiertos	9.1 – 9.10
Acciones	▪ Adquirir un stock suficiente de tarjetas de control de acceso personal para los funcionarios, al igual que mejorar el proceso de descuentos de las tarjetas adquiridas con el fin de comprar las tarjetas extraviadas lo más pronto posible.

Cuadro 15. (Continuación)

	Controlar el acceso al área donde está ubicada la campaña Metlife y trasladar a los funcionarios analistas de calidad y el analista de estadística donde está ubicada la campaña Metlife. ▪ Deshabilitar las tarjetas de acceso en el menor tiempo posible de los funcionarios que ya no laboren en la compañía, se debe agilizar el procedimiento de paz y salvo para informar de manera inmediata cuando una persona ya no labora en la compañía. ▪ Actualizar las políticas de seguridad estableciendo el control de acceso autorizado relacionado a los permisos otorgados en el momento de entrega de carnet. ▪ Realizar un diagrama de distribución de cámaras con el fin de ubicar las cámaras de manera efectiva para monitorear y controlar los accesos a áreas sensibles de la compañía. Instalar las cámaras faltantes en áreas donde se manejan datos del titular, por ejemplo en el área donde están ubicados los analistas de calidad. ▪ Deshabilitar los puntos de red de las salas de juntas como los puntos de red que no tiene ningún equipo conectado, incluir un bloqueo de puertos, por ejemplo cuando la dirección mac relacionada al puerto ha cambiado más de una vez. Actualizar las políticas de seguridad de control de acceso involucrando este tipo de restricciones. ▪ Verificar que todo el acceso físico a los dispositivos inalámbricos estén debidamente controlados, dado que algunos *Acces point* no están ubicados en sitios que sean de difícil acceso, se debe cambiar el sitio de aquellos dispositivos en los cuales se identifique algún tipo de riesgo. ▪ Aislar la operación de Metlife preferiblemente usando implementado un control de acceso biométrico para garantizar que solo ingresen personal relacionado a esta área. ▪ Arreglar puertas que en el momento se encuentran dañadas y dan acceso a operaciones que manipulan datos del titular de la tarjeta, no se aplica de manera adecuada las políticas de control de acceso de Intercontact. ▪ Controlar de manera activa el acceso a personal cuando existe un número considerable de individuos en la recepción, evitar el ingreso no controlado de personal por

Cuadro 15. (Continuación)

	un descuido en la recepción o a nivel de vigilancia, esto ocurre cuando va ingresar personal en formación o cuando hay convocatoria masiva para presentar procesos de prueba de ingreso. Estos procedimientos deben ser debidamente documentados para estos casos. ▪ A nivel documental se debe completar las políticas indicando que en el momento de registro del personal visitante este siempre debe presentar un documento con foto y con número de identificación, para poderle otorgar un carnet de visitante. Fortalecer el procedimiento de devolución de carnet de visitante, porque en el momento de que la persona se lleve este documento podría volver a ingresar por que su reporte no está muy bien definido ▪ Documentar en las políticas el uso del libro de registro en la recepción, indicando cuales son los campos que debe diligenciar. Completar el registro de acceso indicando la persona o funcionario que autoriza su ingreso y quien realizara el acompañamiento permanente del mismo, la empresa de donde proviene y los motivos por los cuales desea ingresar a Intercontact. Este registro debe permanecer por lo menos tres meses disponibles para su debida consulta. ▪ Realizar el debido *backup* de la NAS de la sede de Calle 63 a la sede de Zona franca de los datos del titular de la tarjeta alojados en las bases de datos y grabaciones para garantizar el almacenamiento del *backup* en un lugar que no sea a nivel local. Se deben aplicar prácticas de *hardening* en los servidores NAS con el fin de realizar el almacenamiento en un sitio seguro, también se recomienda realizar auditorías a este mismo servidor con el fin de garantizar la efectividad de los controles. ▪ Actualizar inventario de activos, inventariando y clasificando las grabaciones que contiene datos del titular de la tarjeta como confidencial así mismo el CD utilizado para guardar y enviar esta información al cliente, las bases de datos e informes que se envían también se deben clasificar como confidencial para generar el debido ciframiento de esta documentación o fortalecer la herramienta como el uso de un SFTP o un FTPS. ▪ Involucrar en el procedimiento de traslado de información la debida aprobación desde una dirección o desde la gerencia del transporte del CD enviado y que se realice un

Cuadro 15. (Continuación)

	correcto seguimiento del medio. Se debe contar con un registro de todos los CD enviados al cliente para llevar a cabo su debido control.
Recursos	Recursos económicos, recurso humano
Tiempo	2 Meses
Responsables	Líder Administrativo, Líderes de Operaciones, Director de Tecnología, Director de recursos humanos
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Involucrar un método que pueda demostrar la caducidad de este carnet de visitante, muchas compañías optan por el uso de un sticker impreso con foto, número de identificación y caducidad.
- Utilizar siempre una empresa de envíos para enviar la información en el CD con datos del titular de la tarjeta, con esto se puede realizar un registro de seguimiento de este medio.

11.10 RASTREE Y SUPERVISE TODOS LOS ACCESOS A LOS RECURSOS DE RED Y A LOS DATOS DEL TITULAR DE LA TARJETA

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 10 de la PCI DSS, semuestra a continuación. Ver Cuadro 16.

Cuadro 16. Rastreo y supervisión de todos los accesos de recursos de red y datos del titular de la tarjeta

Objetivo	Rastrear y supervisar todos los acceso a los recursos de red y a los datos del titular
Requerimientos cubiertos	10.1 – 10.9
Acciones	▪ Configurar los registros en los sistemas que están relacionados con el entorno de los datos del titular de la tarjeta, los siguientes: Configurar y habilitar la gestión de *logs*. El registro de acceso de todos los usuarios a los datos del titular en la tarjeta. Usuarios que utilizan cualquiera de los servicios o entran directamente al servidor.

Cuadro 16. (Continuación)

	Registro de los eventos y clasificar estos como un tipo de evento especifico. Registros de entrada como fecha y hora Registros de entrada indicando el éxito o fallo, por ejemplo en el ingreso a algún servicio, servidor o aplicación. El origen de los eventos en la entrada de registros. La identidad o nombre de los datos, de los componentes del sistema o los recursos afectados. El registro de aumento de privilegios de alguna cuenta, la eliminación, creación de cuentas de usuarios que cuenten con privilegios administrativos o raíz La verificación de inicialización, detención o pausa de los *logs*. El registro de todas las creaciones o eliminaciones de objetos a nivel del sistema, para evitar por ejemplo la instalación de algún tipo de *software* malicioso o *malware*. Restringir el acceso para que solo el administrador del sistema pueda ejecutar este tipo de actividad, se deben incluir mecanismos de control de acceso. Establecer parámetros para que estos *logs* estén protegidos, sean seguros y no se puedan modificar Estos registros de deben configurar en los siguientes sistemas: Aplicaciones web Bases de datos Servidor de Telefonía Servidor de Aplicaciones Servidor NAS Configurar los registros que a la fecha no se estén llevando en el Directorio Activo Solicitar al cliente de Metlife que gestione los *logs* de los aplicativos que se tiene con Intercontact como son: FTP VPN ▪ Garantizar que todos los accesos a los diferentes sistemas este vinculados usuarios específicos, no utilizar usuarios genéricos. ▪ Se debe involucrar el registro de todas las cuentas de usuarios administradores de los sistemas, cuentas de usuario con privilegios de *root* o sudo. ▪ Los *logs* deben estar disponibles únicamente para las personas específicas como los administradores, para que

Cuadro 16. (Continuación)

	estos registros no sean modificados por una persona malintencionada. El acceso a estos *logs* también deben quedar registrados. ▪ Configurar en todos los sistemas el registro de accesos lógicos no validos con el fin de identificar por ejemplo ataques de fuerza bruta. ▪ Configurar la fecha y hora con algún servidor NTP o con el servidor de dominio como los otros servidores, los servidores que cuentan con S.O Linux, para que estén sincronizados como los otros sistemas. ▪ Configurar todos los sistemas para que registren en sus *logs* de eventos los cambios en la configuración de la hora y estos se supervisen y revisen. ▪ Configurar los *backups* de los *logs* del directorio activo para que solo sean visibles por el administrador del sistema ya que este *backup* también se guarda otro servidor. Cuando se configure los demás sistemas para que generen *logs* de auditoria se debe limitar la visualización de estos *logs* solo a funcionario que por cuestiones laborales necesitan visualización de los mismos. ▪ Se recomienda guardar los *logs* de equipos como el *Firewalls* y el servidor DMZ que tienen acceso a redes externas y realizar la copia de sus registros en un servidor centralizado como el servidor NAS para evitar riesgo de pérdida o modificación. ▪ Implementar políticas o procedimientos que establezca los siguientes criterios: La revisión al menos una vez al día los eventos de seguridad, los registros de datos del titular, datos confidenciales de autenticación, registros de todos los componentes críticos del sistema y registros de los servidores que realizan funciones de seguridad, ya sea con herramientas manuales de registro. Revisiones periódicas de los registros de los demás componentes del sistema de acuerdo con la evaluación de riegos detectados en la organización Establecer actividades para realizar los debidos seguimientos de las excepciones y anomalías detectadas en el proceso de revisión. Establecer la retención de registros de auditoria por lo menos un año.

Cuadro 16. (Continuación)

	▪ Incluir en el formato de procedimiento de incidencia la restauración de funciones de seguridad, realizar evaluación de riesgos para determinar si se requiere más acciones como resultado de la falla de seguridad. ▪ Establecer una política que indique el monitoreo de todos los accesos a los recursos de la red y a los datos del titular de la tarjeta. Esta política se debe divulgar y debe ser de conocimiento de todas las partes afectadas.
Recursos	Recurso Humano, Recursos económicos para adquisición e implementación de herramientas
Tiempo	1 Meses y 15 días
Responsables	Administradores de plataformas tecnológicas, Director de tecnología, Director de Desarrollo, DBA, Desarrollador, Líder del sistema integrado de gestión.
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Se debe configurar por ejemplo registros en las bases de datos con el fin de identificar la creación o eliminación de tablas o procedimientos almacenados.
- Configurar los *backups* de los *logs* del directorio activo para que solo sean visibles por el administrador del sistema ya que este *backup* también se guarda en otro servidor y este servidor es proporcionado por un proveedor externo y este también tiene acceso al servidor. Esta configuración también debe aplicar en los demás sistemas que se configuren para que proporcione *logs* de auditoria. En la configuración de los *backups* se recomienda que se realice de manera automática como los del directorio activo y en servidores de registros centralizados y que estén configurado para que estos sean difíciles de alterar.
- Se recomienda utilizar técnicas para garantizar la integridad de los archivos o la detección de los cambios en los registro, por ejemplo el uso de *hash* en el archivo de *logs* este puede ser con SHA1 o superior o utilizar herramientas como:
  Algunas de las soluciones comerciales (licenciadas) que proporcionan monitorización de integridad son las siguientes:
  TripWire File Integrity Monitor
  McAfee Integrity Control
  CimTrak File Integrity Monitoring
  Qualys
  NetWrix Auditor
  Verisys File Integrity Monitoring system

Soluciones *open source* como:

OSSEC
Samhain + *Beltane*
Integrit
AIDE
AFICK

- Se recomienda la implementación de herramientas para el análisis de registros como un SIEM como un OSIM, la instalación de un IDS por ejemplo un *Snort*, realizar la configuración de políticas y alertas en estos dispositivos para hacer revisiones más adecuadas.
- La revisión de los eventos de seguridad, los registros de datos del titular, datos confidenciales de autenticación, registros de todos los componentes críticos del sistema y registros de los servidores que realizan funciones de seguridad Este monitoreo se puede realizar con una herramienta de correlacionador de eventos como un OSSIM o ArcSight

11.11 PRUEBE CON REGULARIDAD LOS SISTEMAS Y PROCESOS DE SEGURIDAD

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 11 de la PCI DSS, se muestra a continuación. Ver Cuadro 17.

Cuadro 17. Prueba de los sistemas y procesos de seguridad

Objetivo	Probar con regularidad los sistemas y procesos de seguridad.
Requerimientos cubiertos	11.1 – 11.6
Acciones	▪ Implementar políticas o procedimientos que defina la revisión trimestralmente puntos de acceso inalámbrico autorizado y no autorizados. Se pueden incluir los métodos como análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos configurando las respectivas alertas. Incluir al menos lo siguiente: - Tarjetas WLAN insertadas en los componentes del sistema - Dispositivos portátiles o móviles conectados a los componentes del sistema para crear puntos de acceso inalámbricos (por ejemplo, mediante USB, etc.). - Dispositivos inalámbricos conectados a un puerto o a un

Cuadro 17. (Continuación)

	dispositivo de red. ▪ Verificar que el inventario de activos se mantenga actualizado. ▪ Involucrar de manera específica en el uso de dispositivos móviles la prohibición de generar puntos de acceso inalámbricos no autorizados. ▪ Actualizar los indicadores de seguridad indicando que los análisis de vulnerabilidades ejecutados semestralmente, se ejecuten trimestralmente, que también se realicen después de un cambio significativo de la red y que se incluya un proceso de repetición de los análisis para verificar que se hayan solucionado todas las vulnerabilidades clasificadas con alto riesgo. ▪ Realizar análisis de vulnerabilidades cuando se realicen cambios significativos a nivel de infraestructura o red o el análisis de los componentes del sistema que haya tenido cambios. ▪ Realizar pruebas de *pentest* en la infraestructura relacionada al entorno de los datos de la tarjeta, estas pruebas deben cumplir con enfoques de *pentest* aceptados por la industria. Se debe incluir pruebas a nivel interno y externo de red, pruebas en la capa de aplicación, capa de red, sistemas operativos. Las pruebas de *pentest* internas y externas se deben ejecutar por lo menos una vez al año y después de implementar un cambio o actualización significativa en la infraestructura o aplicaciones relacionadas con el entorno de datos del titular de la tarjeta, este proceso lo debe ejecutar personal calificado ya sea escogido a nivel interno o ejecutado por una entidad externa. ▪ Incluir la revisión y la evaluación de las amenazas y vulnerabilidades ocurridas o detectada en los últimos 12 meses. Documentar todos los resultados de las pruebas de *pentest* y las actividades de corrección de los mismos. ▪ Cuando se detecten vulnerabilidades en las pruebas de *pentest* internas o externas ejecutadas, estas se deben solucionar y se deben repetir las pruebas con el fin de verificar la respectiva corrección. ▪ Ejecutar segmentación en las redes para aislar el entorno de datos del titular de la tarjeta. Realizar pruebas de *pentest* con el fin de validar y verificar que todos estos procesos de segmentación o controles son operativos y

Cuadro 17. (Continuación)

	eficaces y que realmente si se está aislando de alguna manera los entornos de los datos del titular de la tarjeta del resto de entornos. Estas pruebas se deben ejecutar al menos cada seis meses o después de cualquier cambio significativo. ▪ Instalar o configurar un dispositivo IDS, verificar que las políticas de IPS configuradas en el *firewalls* cubran el entorno de datos del titular de la tarjeta y cumpla con el bloqueo de firmas necesarias. ▪ Utilizar técnicas para garantizar la integridad de los archivos críticos del sistema, archivos de configuración o de contenidos por ejemplo con el uso de hash en el archivo de *logs* este puede ser con SHA1 o superior. Se debe ejecutar por lo menos una vez por semana mediante el *software* la comparación de archivos críticos. Actualizar políticas o procedimiento en busca de formalizar este procedimiento. ▪ Actualizar el procedimiento de gestión de cambios o las políticas con el fin de involucrar el proceso para responder a las alertas que se generen en las herramientas implementadas para controlar los cambios, el análisis de vulnerabilidades y pruebas de *pentest* como lo establece la norma.
Recursos	Recursos económicos para la adquisición de herramientas que proporcione la monitorización de la integridad, implementación de IDS y recursos para ejecutar pruebas de *pentest*, Recurso humano
Tiempo	3 Meses
Responsables	Director de tecnología, Administradores de plataformas, profesionales seguridad informática
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Verificar que el asesor externo que realiza el análisis de vulnerabilidades externas cumple con los siguientes requisitos:

  Requerimientos de negocio: En los cuales se evalúa la estabilidad, independencia y cubrimiento por parte de pólizas de seguro de la empresa.
  Requerimientos de capacidad: En los que se revisa la experiencia de

la empresa y del encargado de realizar los escaneos (s*canning operation technical man*ager).
Requerimientos administrativos: En la que se revisa si se cuenta con la logística necesaria para ejecutar los escaneos, incluyendo verificación de antecedentes, cumplimiento con los procedimientos del PCI SSC, controles de calidad y protección de información confidencial y sensitiva proveniente de los resultados del ejercicio.
Requerimientos para el mantenimiento de la certificación: En los cuales se definen los criterios anuales a ser cumplidos para mantener la credencial por parte de la empresa.*"*[2]

- Las pruebas de *pentest* deben cumplir con enfoques de *pentest* aceptados por la industria como por ejemplo basarse en la norma NIST SP800-115 Guía técnica de pruebas de seguridad de la información y evaluación.
- Se recomienda incluir en las políticas o procedimientos la ejecución de pruebas de *pentest* internas y externas con el fin de establecer formalmente actividades, responsables e indicadores de medición.
- Se recomienda trasladar a la red de Metlife al persona de estadística y analista de calidad para aislarlos de otras redes, lo mismo se recomienda aislar de manera lógica los servidores que prestan servicios de Metlife de otras campañas o implementar la autenticación de múltiples factores, ya sea al iniciar sesión en la red del CDE o al iniciar sesión en un sistema. Luego de esto realizar pruebas de *pentest* con el fin de validar y verificar que todos estos procesos de segmentación o controles son operativos y eficaces y que realmente si se está aislando de alguna manera los entornos de los datos del titular de la tarjeta del resto de entornos.
- Instalar un dispositivo IDS como por ejemplo un *Snort* y configurar las diferentes reglas para detectar las diferentes amenazas que se presenten en el perímetro del titular de la tarjeta y generar las respectivas alertas. Estos sistemas se debe actualizar con frecuencia las bases y firmas. Este dispositivo debe ser instalado en un lugar que pueda monitorear todo el perímetro y puntos críticos del entorno de datos del titular de la tarjeta.

11.12 MANTENGA UNA POLÍTICA QUE ABORDE LA SEGURIDAD DE LA INFORMACIÓN PARA TODO EL PERSONAL

El plan de acción que se llevará a cabo para dar cumplimiento al requisito 12 de la PCI DSS, se muestra a continuación. Ver Cuadro 18.

[2] PCI HISPANO. Criterios para escoger un Proveedor Aprobado de Escaneo (ASV). 2016. Disponible en: pcihispano.com

Cuadro 18. Mantenimiento de política de seguridad para todo el personal

Objetivo	Mantener una política que aborde la seguridad de la información para todo el personal de Intercontact.
Requerimientos cubiertos	12.1 – 12.11
Acciones	▪ Verificar si los proveedores, contratistas o terceros nuevos de la compañía tienen conocimiento de las políticas de seguridad de la compañía. ▪ Verifique que las políticas hayan sido revisadas y exista evidencia física o digital de esto. ▪ Identificar que el tratamiento de riegos y la evaluación de los riesgo se esté realizando de acuerdo al procedimiento establecidos por Intercontact. ▪ Actualizar las políticas de seguridad sobre el uso de dispositivos móviles involucrando aspectos relacionados con las laptos ya que a la fecha no se tienen en cuenta sobre su uso y restricciones. ▪ Cada vez que sean aprobadas y actualizadas las políticas de seguridad estas deben ser informadas a todos los funcionarios y partes interesadas para ejercer el debido cumplimiento de las mismas. ▪ Identificar si se requiere la implementación de otros métodos de autenticación en las políticas por ejemplo el uso de *tokens*, dependiendo de la tecnología o a la información a la que se requiere acceder. ▪ Verificar si todos los dispositivos están listados en el inventario de activos con su debida clasificación. Se debe listar todo el personal autorizado para utilizar los dispositivos y este debe ser revisado y actualizado con frecuencia. ▪ Actualizar periódicamente el inventario de activos, además de agregar campos como por ejemplo propietario y contacto cuando aplique. Se debe identificar el uso de equipos o dispositivos que no estén debidamente etiquetados e inventariados. Se sugiere emplear un etiquetado lógico con el cual se determine con el código aspectos como: tipo de dispositivo, propietario, tipo de información, etc. ▪ Verificar las políticas de seguridad de la Información e involucrar los siguientes aspectos: Implementar en las que se crea pertinente el uso aceptable de la tecnología. Involucrar en las políticas relacionadas a uso de dispositivos móviles y de red la definición de las

Cuadro 18. (Continuación)

	ubicaciones aceptables de la tecnología en la red. Incluir una lista de los productos aprobados por la empresa, identificado la tecnología aprobada por la compañía, con el fin de asegurar que no se abran brechas de seguridad. En las políticas de teletrabajo, políticas de control de acceso a la información o política de desarrollo se involucre la desconexión automática de las sesiones en las tecnologías de acceso remoto después de un periodo específico de inactividad. Involucrar la activación de accesos remotos solo cuando se necesiten y que se desactiven automáticamente después de usarlas. Involucrar la prohibición de copiar, mover o almacenar los datos del titular de la tarjeta alojados en discos locales y en dispositivos electrónicos extraíbles al acceder a dichos datos a través de tecnologías de acceso remoto. Verificar que las configuraciones en los sistemas realicen correctamente estos bloqueos. Estas políticas deben ser aplicadas a todos los funcionarios, terceros y proveedores que prestan sus servicios a Intercontact ▪ Verificar si realmente se estas desactivando los servicios de acceso remoto inmediatamente después de su uso, puede suceder que se otorguen los permisos pero luego no se vuelva hacer gestión de los mismos. ▪ Involucrar en las políticas o en los perfiles de los funcionarios relacionados con el entorno de los datos del titular la responsabilidad general de mantener el cumplimiento con la PCI DSS. La alta dirección debe generar un estatuto u objetivo de cumplimiento de la PCI DSS e informar esto a todos los directivos de la compañía sobre la responsabilidad general de mantener el cumplimiento de la norma en la compañía. ▪ Completar el debido procedimiento de gestión de incidentes con los debidos escalamientos y tiempos de respuesta que debe ser realizados ante un incidente de seguridad para garantizar el manejo efectivo y oportuno de todas las situaciones. ▪ Documentar formalmente que roles específicos del área de tecnología que están encargados de administrar las diferentes cuentas de usuario. Asignar formalmente la responsabilidad de monitorear y controlar el acceso a los

Cuadro 18. (Continuación)

	datos del titular de la tarjeta. ▪ En las formaciones iniciales y las de refuerzo se debe involucrar el cumplimiento de políticas y procedimientos de seguridad relacionados con los datos del titular de la tarjeta en cargos o roles que estén relacionados con el entorno de los datos del titular de la tarjeta. ▪ Se debe documentar formalmente una declaración por lo menos anual de los funcionarios de Intercontact que incluya que leyeron y entendieron las políticas de seguridad de la compañía y están comprometidos con las mismas. ▪ Verificar que proveedores tiene acceso a los datos del titular de la tarjeta y establecer un acuerdo por escrito en el cual los proveedores aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos almacenan o procesan. Entre los proveedores identificados esta Mitrol (telefonía) y *Losytec (Backups*). ▪ Involucrar un proceso de auditoria previa al compromiso con proveedores que van a tener relación con los datos del titular de la tarjeta (almacenamiento, procesamiento y transmisión) o con los proveedores que ya se tiene una relación comercial, esta auditoria debe evaluar aspectos como prácticas de presentación de informes, respuesta ante incidentes, detalles de cómo se asignan responsabilidades de la PCI DSS, cumplimiento con la PCI DSS y que evidencias se presentaran con el fin de dar cumplimiento a PCI DSS ▪ Verificar que servicios ofrece cada proveedor que tenga relación con el almacenamiento, procesamiento o transmisión de información de datos del titular e identificar qué requisitos de la PCI DSS aplican a estos para determinar qué requisitos son administrados por Intercontact y cuales por el proveedor. ▪ Documentar como se relacionan los procedimientos de gestión de incidentes de seguridad y gestión de incidentes en plataformas tecnológicas. Complementar en procedimiento de incidentes en los componentes tecnológicos incluyendo los siguientes aspectos cuando se vea comprometido un sistema que esté relacionado con el entorno de los datos del titular: Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya:

Cuadro 18. (Continuación)

	Análisis de los requisitos legales para el informe de riesgos. Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago. Lecciones aprendidas con el fin ser capaz de reaccionar ante las amenazas emergentes y las tendencias de seguridad. ▪ Involucrar en el plan de continuidad aspectos como: Análisis de los requisitos legales para el informe de riesgos. Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago. ▪ Implementar sistemas como IDS, IPS, smtp del *firewalls* para que genere alertas al nagios y sistemas de integridad de archivos que genere alertas sobre los sistemas involucrados en el entorno de datos del titular de la tarjeta e involucre procedimientos de observación y revisión de estos sistemas y que los planes de respuesta ante incidentes se inicien cuando se presente un incidente. ▪ Documentar las revisiones que se realiza sobre el sistemas sobre los procedimientos, configuraciones y políticas establecidos por la PCI DSS
Recursos	Recursos económicos para equipos de monitoreo, recurso humano
Tiempo	2 Meses
Responsables	Líder del sistema integrado de gestión, oficial o líder de seguridad de la información, Director de tecnología, Director de Formación
Fuente: Elaboración propia, 2017	

RECOMENDACIONES

- Solicitar al cliente Metlife la desactivación de sesiones cuando pase un lapso de tiempo determinado de las aplicaciones como VPN y FTP.
- En algunos casos cuando un funcionario empieza en la compañía no se realiza la debida formación relacionada a aspectos de seguridad que debe tener en cuenta en su cargo específico. Se debe involucrar en la formación del cargo aspectos de cumplimiento con la seguridad de la información.
- Implementar sistemas de información que monitoree y analice alertas como es un correlacionador de eventos como un OSSIM o un ArcSight, IDS como un Snort, etc.
  Estos dispositivos se deben configurar de manera que genere las debidas alertas y que estas sean analizadas y que sean comunicadas al personal que se hay

asignado formalmente.

- Se sugiere asignar el rol de monitorear y controlar el acceso a los datos del titular de la tarjeta a alguno del *help desk* de tecnología
- Revisar que proveedores tienen acceso o se comparten información de datos del titular, por ejemplo *Mitro*l y *losytec* verificar que estos estén cumpliendo con todas las políticas y procedimientos de la compañía y limitar el acceso a los datos en el mayor grado posible.
- Verificar que la lista de proveedores se mantenga actualizada y que en todos se involucre una descripción del servicio prestado, cada vez que ingresa un proveedor nuevo o se elimine un proveedor, a algún dato cambie con este proveedor (razón social, procesos, etc).
- Verificar que la compañía si tiene por escrito mantener los requisitos correspondientes de la PCI DSS con Metlife.
- Informar a los funcionarios o partes interesadas los procedimientos de gestión de incidentes que tiene intercontact para evitar periodos de inactividad más prolongados para el negocio, responsabilidades legales y exposición innecesaria de medios al público.
- Involucrar en las políticas o en las funciones de los perfiles específicos del proceso de tecnología, la disponibilidad de funcionarios las 24 horas 7 días a la semana, entre las funciones también se debe incluir la respuesta ante incidentes, el monitoreo de la cobertura de cualquier evidencia de actividad no autorizada, detección de puntos de acceso inalámbricos no autorizados, alertas críticas de por ejemplo un IDS o informes de cambios no autorizados en archivos de contenido o de sistemas críticos.
- Evidenciar de manera formal o documental que todos los funcionarios de tecnología fueron capacitados ante las responsabilidades, criterios de comunicación y respuestas que deben ejecutar ante alguna falla de seguridad.
- Involucrar las revisiones de las alertas de seguridad de los sistemas que tiene relación con el entorno de los datos del titular al menos trimestralmente.

11.13 ADQUISICIONES O COMPRAS (Cotizaciones)

HSM

Hardware Security Module (Módulo de Seguridad Hardware). HSM Es un dispositivo criptográfico que genera, almacena y protege claves criptográficas, y aporta aceleración hardware para operaciones criptográficas maximizando el rendimiento de las aplicaciones, otorgando protección a las transacciones y prestando servicios de cifrado, descifrado, autenticación y firma digital. Ver Tabla 2.

Tabla 2. Precio Hsm profesional

Producto	Precio
Hsm Professional	$8920 Perpetua $2765 Anual
Fuente: Elaboración propia, 2017	

Algunas de las soluciones comerciales (licencias) que proporcionan monitorización de integridad son las siguientes:

- ***NetWrix Auditor for Active Directory***

Permite a los administradores y profesionales de seguridad supervisar e informar sobre cambios en el directorio activo incluyendo quien cambio algo, cuando lo cambio, y de que estación.

A parte de los manejos de cambio también ofrece una herramienta para hacer reportes para el directorio activo y políticas de grupo.
Tiene la habilidad de recuperar cambios sin autorización donde los objetos del directorio activo fueron borrados. También puede mostrar los resultados de un cambio antes que el cambio sea realizado.
Incluye reportes predeterminados, como incluyendo reportes de auditoria regulatoria para PCI, HIPAA, SOX y FISMA. Ver Tabla 3.

Tabla 3. Precio NetWrix Auditor

Producto	Precio
NetWrix Auditor	$1,549 para 149 o menos usuarios, por encima de 150 usuarios, cada usuario vale $9.50 adicionales.
Fuente: Elaboración propia, 2017	

- ***Verisys File Integrity Monitoring System***

Detecta cambios no autorizados. Es un Sistema avanzado para Windows, Linux y otros dispositivos de red para mantener la integridad de los archivos y la información al detectar cambios sin autorización.

Permite realizar administración centralizada que consiste en realizar chequeos de integridad, reportes y administración de licencias.

Verisys examina un gran número de propiedades y atributos de cada archivo así como usando criptografía robusta para detectar que cambios han sido hechos.

El sistema enviara automáticamente un correo al personal encargado cuando un cambio sin autorización se haya hecho.

Incluye reportes predeterminados, como incluyendo reportes de auditoria regulatoria para PCI, HIPAA, SOX y FISMA.Ver Tabla 4.

Tabla 4. Precio Verisys File Integrity Monitoring System

Producto	Precio
Verisys File Integrity Monitoring System	$339.99 USD Server/Destock

Fuente: Elaboración propia, 2017

- ***McAfee Integrity Control***

Bloquea aplicaciones sin autorización, así como intentos de cambios.

Monitorea integridad de archivos y cambios de archivo.

Incrementa el control de funciones de sistemas fijos.

Cumple con los requerimientos de PCI, DSS.

Manejo centralizado a través del ePO. Ver Tabla 5.

Tabla 5. Precio McAfee Integryty Control

Producto	Precio
McAfee Integrity Control	$239.24 por un año para un node.

Fuente: Elaboración propia, 2017

- ***TripWire File Integrity Monitor***

Tiene manejo de políticas, manejo de cambios y monitoreo de la integridad del archivo en un solo lugar.

Tiene una biblioteca de más de veinticinco políticas y una combinación de plataformas. Esto incluye lineamientos regulatorios como PCI, HIPAA y NERC, y también lineamientos de proveedores, política de seguridad y estándares específicos de cada país.

Todo el manejo se hace a través de una consola en línea para un control más fácil para el administrador. Ver Tabla 6.

Tabla 6. Precio TripWire File Intgrity Monitor

Producto	Precio
TripWire File Integrity Monitor	$699 por un node

Fuente: Elaboración propia, 2017

- ***CimTrak File Integrity Monitoring***

Es conocida como una alternativa de *TripWire File Integrity Monitor* más económica.

CimTrak File Integrity Monitoring tiene un sistema de proceso de detección automático, capacidad de auditoria, protege cualquier tipo de archivo, documentos, aplicaciones etc.

Ofrece monitoreo integral a todo el ambiente de IT, reúne los requerimientos de PCI, DSS.

Es la única herramienta autorizada para ser usada en el Departamento de Defensa de los Estados Unidos.Ver Tabla 7.

Tabla 7. Precio CimTrak File Inte4grity Monitoring

Producto	Precio
CimTrak File Integrity Monitoring	$ 209.77

Fuente: Elaboración propia, 2017

- ***Qualys Continuous Monitoring***

Es un servicio en la nube que da la habilidad de identificar amenazas y cambios inesperados en su *Network* antes de que se convierta en problemas. La administración tiene acceso desde cualquier parte del mundo.

Es fácil de instalar y monitorea problemas potenciales como *hots* inesperados, certificados SSL a puntos de inspirar, puertos abiertos, vulnerabilidades severas y aplicaciones no deseadas. Ver Tabla 8.

Tabla 8. Precio Qualys Continous Monotorig

Producto	**Precio**
Qualys Continuous Monitoring	$795 Express Lite, por dos internet assets.
Fuente: Elaboración propia, 2017	

- Para dar cumplimiento al requerimiento 11.4 de PCI DSS. Una buena guía de implementación de SNORT para identificar datos de tarjetas de pago se puede encontrar en el siguiente artículo del SANS Institute: "*Using Snort to Detect Clear Text Credit Card Numbers*" http://www.sans.org/security-resources/idfaq/snort-detect-credit-card-numbers.php

12. CRONOGRAMA DE ACTIVIDADES

De acuerdo a los planes de acción se realiza la propuesta de ejecución de actividades que deben ser desarrollas o ejecutadas a lo largo de un periodo aproximado de año y medio, en el cual se establece como fecha de inicio de ejecución de actividades el 01 de Septiembre del 2017 y una fecha de finalización del 03 de mayo del 2019, si bien varias de las fechas de desarrollo de actividades están en desorden o se repiten es porque son ejecutadas por áreas distintas de la compañía o son actividades que pueden ser realizadas independientemente al mismo tiempo.

Si Intercontact en conjunto con sus funcionarios, proveedores, clientes y terceros ejecutan estas actividades como propuestas en los tiempos establecidos se podría decir que a mediados del año 2019 todas actividades relacionadas con el almacenamiento, trasmisión y almacenamiento de los datos del titular de la tarjeta que se realizan en Intercontact cumplirá con todos los controles impuestos por la PCI DSS para la campaña Metlife u otra campaña similar que llegue a la compañía y que se implemente estos controles.

A continuación se muestra el cronograma con las respectivas actividades, responsables, duración en días, fecha de inicio y fin de ejecución y desarrollo de actividades.

Se debe tener presente que en este cronograma no se tuvo en cuenta las actividades mencionadas en las recomendaciones que se realizan en cada plan de acción. Ver Cuadro 19.

Cuadro 19. Cronograma

Actividad	Responsable	Duración	Comienzo	Fin
Crear procedimiento de la configuración del *firewall*	Administrador del *Firewalls*	5 días	vie 9/1/17	jue 9/7/17
Involucrar aprobación y las pruebas para cambios configurados en el *firewall*	Director de Tecnología	2 días	vie 9/8/17	lun 9/11/17
Actualizar el diagrama de red que muestre detalles de la estructura tecnológica a nivel de red LAN	Ingeniero de Infraestructura	2 días	mar 9/12/17	mié 9/13/17
Realizar diagramas de flujo de datos donde se evidencie el flujo de datos de los titulares de las tarjetas.	Ingeniero de Infraestructura y Jefe de Operaciones	5 días	jue 9/14/17	mié 9/20/17
Documentar descripción de roles y responsabilidades de quienes acceden al *firewall*	Director de Tecnología	3 días	jue 9/21/17	lun 9/25/17

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
Definir y documentar todos los servicios, protocolos, puertos, rutas y demás de manera formal y justificada de cada campaña	Director de Tecnología e Ingeniero de Infraestructura	3 días	mar 9/26/17	jue 9/28/17
Revisión de las normas de configuración del *firewall*	Administrador del *Firewalls*	3 días	vie 9/29/17	mar 10/3/17
Verificar que todas las conexiones a la fecha hacia redes no confiables o externas estén debidamente configuradas.	Administrador del *Firewalls*	2 días	mié 10/4/17	jue 10/5/17
Configurar la campaña Metlife para que se restringa la cantidad necesaria de tráfico	Administrador del *Firewalls*	5 días	vie 10/6/17	jue 10/12/17
Se debe configurar el *firewall* para que separe la red de Metlife y la red inalámbrica	Administrador del *Firewalls*	3 días	vie 10/13/17	mar 10/17/17
Generar una tarea (*checklist*) en la que se guarde el archivo de configuración antes de sacar el *backup* del Core.	Ingeniero de Infraestructura	3 días	mié 10/18/17	vie 10/20/17
Denegar o controlar el acceso a internet redes internas que gestionan los datos de las tarjetas y titulares de las tarjetas.	Ingeniero de Infraestructura	3 días	lun 10/23/17	mié 10/25/17
La configuración de las aplicaciones montadas en la DMZ estén con la debida documentación	Administrador del *Firewalls*	4 días	jue 10/26/17	mar 10/31/17
Bloquear o limitar el acceso a internet los analistas de estadística y de calidad.	Administrador del *Firewalls*	2 días	mié 11/1/17	jue 11/2/17
Instalar un *firewall* personal a los equipos móviles corporativos como computadores portátiles	Administrador del *Firewalls*	15 días	vie 11/3/17	jue 11/23/17
Deshabilitar o cambiar las contraseñas predeterminadas de los servidores NAS, de Telefonía, WSUS y los *Acces point*. . Solicitar al cliente que realice cambio periódico de contraseña.	Administradores de plataformas tecnológicas	2 días	vie 11/24/17	lun 11/27/17
Documentar procedimiento sobre configuración de seguridad en los dispositivos de entornos inalámbricos (*Acces point*), servidores, *firewalls*, *switchsv y radius*	Administradores de plataformas tecnológicas y Director de Tecnología	7 días	mar 11/28/17	mié 12/6/17
Implementar *hardening* en todos los servidores que tienen relación con la	Administradores de plataformas tecnológicas y	30 días	jue 12/7/17	mié 1/17/18

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
campaña metlife y estén involucrados con los datos del titular de la tarjeta.	Director de Tecnología			
Configurar aplicaciones para que antes de entrar estas a producción funcionen por tls 1.2 o superior	Administrador de servidor de producción y desarrollador	5 días	jue 1/18/18	mié 1/24/18
Deshabilitar el acceso por http de la consola de administración y aplicaciones de la campaña Metlife.	Administrador de servidor de producción y desarrollador	2 días	jue 1/25/18	vie 1/26/18
Actualizar el inventario de activos existente con todos los componentes relacionados con la campaña metlife y procesos que están involucrados en el CDE	Administradores de plataformas, Director de tecnología, Líderes de mesa de servicio	5 días	lun 1/29/18	vie 2/2/18
Ampliar el detalle de informes de la plataforma google que utiliza Intercontact	Director de Tecnología y Administrador de servicios google para Intercontact	3 días	lun 2/5/18	mié 2/7/18
Determinar y generar un procedimiento y políticas para la limitación de almacenamiento de datos del titular de la tarjeta y retención de los mismos de acuerdo a requisitos legales	Director de Operaciones, Líder del sistema integrado de Gestión	7 días	vie 9/1/17	lun 9/11/17
Establecer un proceso de eliminación segura de datos del titular de la tarjeta cuando estos ya no son necesarios	Director de Operaciones, Líder del sistema integrado de Gestión, Director de Tecnología	7 días	mar 9/12/17	mié 9/20/17
Establecer políticas que indiquen cuales son los únicos valores que pueden ser almacenados en los cuales no puede ser involucrados	Director de Operaciones, Líder del sistema integrado de Gestión	5 días	jue 9/21/17	mié 9/27/17
Generar un documento que estipule las funciones o perfiles que están específicamente autorizadas para ver el número PAN completo	Director de Operaciones, Líder del sistema integrado de Gestión	7 días	vie 9/22/17	lun 10/2/17
Enmascarar u ocultar los seis o los últimos cuatro dígitos del PAN y convertirlo en ilegible para su debido almacenamiento	Director de Tecnología, Administradores de servidor de aplicaciones, DBA y Desarrollador	30 días	jue 2/8/18	mié 3/21/18
Cifrar las bases de datos que contienen datos del titular de la tarjeta con un cifrado fuerte	Director de Tecnología, Administradores de	20 días	jue 3/22/18	mié 4/18/18

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
	servidor de aplicaciones, DBA y Desarrollador			
Se debe establecer procedimientos y políticas para la protección de contraseñas que son usadas para la protección de datos del CDE	Director de Tecnología, DBA, Desarrollador, Líder del Sistema de Gestión de Intercontact	6 días	jue 4/19/18	jue 4/26/18
Establecer protocolos de seguridad con el cliente Metlife para reforzar el acceso a la VPN y el FTP y custodiar las claves de acceso	Director de tecnología, Director de Operaciones, Cliente Metlife	20 días	vie 4/27/18	jue 5/24/18
Cifrar la información que debe ser cifrada de los datos del titular y las claves de cifrado de estas bases	Director de tecnología, Desarrollador, DBA, Administrador de servidor de aplicaciones	20 días	vie 5/25/18	jue 6/21/18
Crear un procedimiento para cifrar la información del titular de la tarjeta y administración de claves utilizadas para cifrar esta información, involucrar plataformas del cliente Metlife y los datos enviados al mismo enviado de manera física	Director de tecnología, Director de Operaciones, Cliente Metlife	7 días	vie 6/22/18	lun 7/2/18
Generar el procedimiento de generación de claves en el cual se debe involucrar aspectos que especifiquen la distribución de claves de manera segura, Las claves de cifrado utilizadas se deben guardar de manera segura.	Director de Tecnología, Director de Operaciones, Cliente Metlife, Líder del sistema integrado de gestión	7 días	mar 7/3/18	mié 7/11/18
Desarrollar procedimiento de gestión de claves	Director de tecnología, director de operaciones, líder del sistema integrado de gestión, director de desarrollo	7 días	mié 7/12/17	jue 7/20/17
Completar las políticas de seguridad de la información con aspectos detallados sobre la protección de datos del titular de la tarjeta	Director de tecnología y desarrollo, director de operaciones, líder del sistema integrado de gestión	5 días	lun 7/23/18	vie 7/27/18

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
El servidor FTP de Metlife debe tener una configuración de seguridad adecuada	Director de Operaciones, Cliente Metlife	7 días	mar 10/3/17	mié 10/11/17
Documentar políticas y procedimientos que establezca la configuración segura para el transporte seguro de información	Director de tecnología, Director de Operaciones, Líder del sistema Integrado de gestión.	7 días	lun 7/30/18	mar 8/7/18
Se debe configurar la aplicación Web que se usa a nivel LAN con https y habilitar TLS 1.2 o superior	Administrador del servidor de aplicaciones, Desarrollador.	3 días	mié 8/8/18	vie 8/10/18
Genere la debida documentación y procedimientos para el debido acceso y configuración de un equipo a la red inalámbrica, protocolos, mejores prácticas entre otros.	Director de tecnología, Ingeniero de Infraestructura	7 días	lun 8/13/18	mar 8/21/18
Cifrar el numero PAN en las transmisiones de este por el FTP o el aplicativo web y la documentación legalizando el procedimiento	DBA, Desarrollador, Ingeniero de Infraestructura, Director de Tecnología	15 días	mié 8/22/18	mar 9/11/18
Implementar procedimientos y políticas que establezcan que los datos del titular de la tarjeta sean cifrados en las transmisiones	Director de Tecnología, Director de Operaciones, Director de Desarrollo, Líder del sistema de gestión	5 días	mié 9/12/18	mar 9/18/18
Definir la periodicidad para la ejecución de análisis del antivirus en los equipos y servidores de la compañía	Director de tecnología, Administrador de consola de Antivirus	3 días	mié 9/19/18	vie 9/21/18
Definir procedimientos documentados que establezcan las actividades que se deben llevar a cabo cuando es necesario desactivar la protección del antivirus	Director de tecnología, Administrador de consola de Antivirus	7 días	lun 9/24/18	mar 10/2/18
Revisar criterios para la evaluación de las vulnerabilidades y asignar la clasificación de riesgo a esas vulnerabilidades	Líder de seguridad de la información, director de tecnología	2 días	mié 10/3/18	jue 10/4/18
Involucrar en las políticas de Intercontact la instalación de parches que deben ser aplicados tanto en estaciones de trabajo como en servidores	Líder de seguridad de la información, director de tecnología, Administradores de servidores	3 días	vie 10/5/18	mar 10/9/18

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
Involucrar formalmente la seguridad de la información durante todo el ciclo de vida del *software*	Director de desarrollo, DBA, Administrador de servidor de aplicaciones	7 días	mié 10/10/18	jue 10/18/18
Bloquear los respectivos accesos del desarrollador al ambiente de producción	Administrador de servidor de aplicaciones	1 día	vie 10/19/18	vie 10/19/18
Ampliar alcance y actividades del procedimiento de gestión de cambios	Director de tecnología y Director de desarrollo	2 días	lun 10/22/18	mar 10/23/18
Complementar todo el procedimiento de desarrollo e implementarlo	Director de desarrollo, DBA, Administrador de servidor de aplicaciones	30 días	mié 10/24/18	mar 12/4/18
Actualizar indicadores de solución de vulnerabilidades	Líder de seguridad de la información	4 días	mar 10/10/17	vie 10/13/17
Definir, establecer y documentar parámetros más restrictivos a la información que accede los funcionarios de la compañía, definición por cargos y funciones	Director de operaciones, Director de tecnología, Director de desarrollo, Líder del sistema integrado de gestión	10 días	jue 10/25/18	mié 11/7/18
Complementar el procedimiento de asignación de roles y privilegios	Director de tecnología, Administradores de Plataformas	3 días	jue 11/8/18	lun 11/12/18
Reforzar el procedimiento de creación, modificación y eliminación de usuarios	Director de tecnología, Administradores de Plataformas	2 días	mar 11/13/18	mié 11/14/18
Solicitar al cliente Metlife la creación de perfiles con respectivo ID y usuario	Director de Operaciones	1 día	lun 10/16/17	lun 10/16/17
Establecer horarios de acceso a los proveedores con el fin que solo se use cuando en el horario establecido y se deshabiliten automáticamente. Además se debe definir el nivel de acceso que tienen estos a la información y a los sistemas.	Director de Tecnología y Administradores de Plataformas	2 días	jue 11/15/18	vie 11/16/18
El procedimiento de gestión de usuarios y contraseñas debe regir en todos los sistemas que involucran los datos del titular de la tarjeta	Director de Tecnología y Administradores de Plataformas	3 días	lun 11/19/18	mié 11/21/18

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
Actualizar las políticas o procedimientos relacionados a temas de identificación y autenticación	Director de Tecnología, Director de Operaciones, Administradores de plataformas, Líder del sistema integrado de gestión	15 días	jue 11/22/18	mié 12/12/18
Implementar autenticación de doble factor a nivel de acceso administrativo individual que no sea de consola y todo acceso remoto, el acceso a la bases de datos y a la grabaciones que contiene datos del titular de la tarjeta	Director de Tecnología y Administradores de Plataformas	30 días	jue 12/13/18	mié 1/23/19
Se debe deshabilitar el usuario administrativo	Administradores de plataformas	1 día	jue 1/24/19	jue 1/24/19
Realizar configuraciones para que solo el administrador de la base de datos sea el único que puede acceder directamente a la base de datos para realizar consultas	Administradores de plataformas, Desarrollador y DBA	3 días	vie 1/25/19	mar 1/29/19
Controlar el acceso al área donde está ubicada la campaña Metlife y adquirir un *stock* de tarjetas, agilizar procedimiento de paz y salvo	Líder Administrativo, Directo de recursos humanos, Director de Operaciones	2 días	mar 10/17/17	mié 10/18/17
Realizar un diagrama de distribución de cámaras e instalar cámaras faltantes	Líder Administrativo, Director de Tecnología, Líder de Seguridad	8 días	mié 10/18/17	vie 10/27/17
Deshabilitar los puntos de red que no se usan y bloquear otros con ciertos parámetros de uso	Ingeniero de Infraestructura	1 día	mié 1/30/19	mié 1/30/19
Verificar que todo el acceso físico a los dispositivos inalámbricos estén debidamente controlados	Ingeniero de Infraestructura, Director de tecnología	2 días	jue 1/31/19	vie 2/1/19
Aislar la operación de Metlife preferiblemente usando implementado un control de acceso biométrico	Líder Administrativo, Director de operaciones	10 días	lun 10/30/17	vie 11/10/17
Arreglar puertas que en el momento se encuentran dañadas y dan acceso a operaciones que manipulan datos del titular de la tarjeta	Líder Administrativo, Director de operaciones	15 días	lun 11/13/17	vie 12/1/17

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
Actualizar documentación relacionada al control de acceso en la recepción	Líder Administrativo, Líder de seguridad	7 días	lun 12/4/17	mar 12/12/17
Realizar el debido *backup* de la NAS de la sede de Calle 63 a la sede de Zona franca de los datos del titular de la tarjeta	Director de Tecnología, Administrador de servidor NAS	15 días	lun 2/4/19	vie 2/22/19
Actualizar el procedimiento de traslado de información	Director de Operaciones, Líder de Seguridad	2 días	mié 12/13/17	jue 12/14/17
Configurar los registros en los sistemas que están relacionados con el entorno de los datos del titular de la tarjeta	Administradores de plataformas, DBA, Desarrollador, Director de Tecnología, Director de Desarrollo	20 días	lun 2/25/19	vie 3/22/19
Registro de todas las cuentas de usuarios administradores de los sistemas, cuentas de usuario con privilegios de root o sudo.	Administrador de plataformas	2 días	lun 3/25/19	mar 3/26/19
Configuración de políticas de *logs*	Director de tecnología, Administradores de plataformas	10 días	mié 3/27/19	mar 4/9/19
Actualizar procedimiento de incidencias de tecnología	Director de tecnología, Líder de mesa de ayuda	1 día	mié 4/10/19	mié 4/10/19
Configurar NTP	Administradores de plataformas	8 días	jue 4/11/19	lun 4/22/19
Política de monitoreo de acceso	Director de tecnología, Administradores de plataformas	3 días	mar 4/23/19	jue 4/25/19
Implementar políticas o procedimientos que defina la revisión trimestralmente puntos de acceso inalámbrico autorizado y no autorizados	Director de tecnología, Ingeniero de Infraestructura	3 días	vie 4/26/19	mar 4/30/19
Actualizar los indicadores de seguridad relacionado a la solución de vulnerabilidades y ejecutar los debidos análisis	Líder de seguridad de la información o informática	15 días	vie 12/15/17	jue 1/4/18
Realizar pruebas de *pentest* en la infraestructura relacionada al entorno de los datos de la tarjeta	Líder de seguridad de la información o informática	10 días	vie 1/5/18	jue 1/18/18

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
Ejecutar segmentación en las redes para aislar el entorno de datos del titular de la tarjeta y ejecutar las respectivas pruebas de *pentest*	Líder de seguridad de la información o informática, Ingeniero de infraestructura	8 días	vie 1/19/18	mar 1/30/18
Instalar o configurar un dispositivo IDS, verificar que las políticas de IPS configuradas en el *firewall* cubran el entorno de datos del titular de la tarjeta	Líder de seguridad de la información o informática, Ingeniero de infraestructura	30 días	mié 1/31/18	mar 3/13/18
Utilizar técnicas para garantizar la integridad de los archivos críticos del sistema contenidos por ejemplo con el uso de hash en el archivo de *logs*	Líder de seguridad de la información o informático, administrado de la plataforma de integridad de archivos	30 días	mié 3/14/18	mar 4/24/18
Actualizar el procedimiento de gestión de cambios o las políticas con el fin de involucrar el proceso para responder a las alertas que se generen en las herramientas implementadas	Director de tecnología, administradores de plataformas de seguridad	4 días	mar 4/30/19	vie 5/3/19
Verifique que las políticas hayan sido revisadas, actualizadas e involucre los aspectos descritos a lo largo del documento. Los proveedores, terceros y funcionarios las conozcan y debe estar formalmente documentado que conocen y entienden las políticas	Líder del sistema integrado de gestión, líder de seguridad de la información	20 días	mié 4/25/18	mar 5/22/18
Verificar si realmente se estas desactivando los servicios de acceso remoto inmediatamente después de su uso	Ingeniero de infraestructura	2 días	mié 5/23/18	jue 5/24/18
La alta dirección debe generar un estatuto u objetivo de cumplimiento de la PCI DSS e informar esto a todos los directivos de la compañía	Alta dirección	1 día	vie 5/25/18	vie 5/25/18
Completar el debido procedimiento de gestión de incidentes con los debidos escalamientos y tiempos de respuesta	Líder de seguridad de la información	3 días	lun 5/28/18	mié 5/30/18

Cuadro 19. (Continuación)

Actividad	Responsable	Duración	Comienzo	Fin
Documentar formalmente que roles específicos del área de tecnología que están encargados de administrar las diferentes cuentas de usuario	Director de tecnología	1 día	jue 5/31/18	jue 5/31/18
En las formaciones iniciales y las de refuerzo se debe involucrar el cumplimiento de políticas y procedimientos de seguridad relacionados con los datos del titular de la tarjeta	Director de formación	3 días	vie 6/1/18	mar 6/5/18
Verificar que proveedores tiene acceso a los datos del titular de la tarjeta y establecer un acuerdo por escrito en el cual los proveedores aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta	Líder de seguridad de la información	5 días	mié 6/6/18	mar 6/12/18
Involucrar un proceso de auditoria previa al compromiso con proveedores que van a tener relación con los datos del titular de la tarjeta o que ya tiene una relación con los mismos	Líder de seguridad de la información	10 días	mié 6/13/18	mar 6/26/18
Determinar qué requisitos son administrados por Intercontact y cuales por el proveedor.	Director de tecnología y Líder administrativo	3 días	mié 6/27/18	vie 6/29/18
Documentar como se relacionan los procedimientos de gestión de incidentes de seguridad y gestión de incidentes en plataformas tecnológicas	Líder de seguridad de la información, Líder de gestión de incidentes, Director de tecnología	3 días	lun 7/2/18	mié 7/4/18
Actualizar plan de continuidad del negocio	Líder de seguridad de la información	5 días	jue 7/5/18	mié 7/11/18

Fuente: Elaboración propia, 2017

13. CONCLUSIONES

- Intercontact cuenta con un gran nivel de documentación de políticas, funciones y procedimientos que fueron creados para la implementación de un sistema de gestión de seguridad de la información que pueden ser aprovechados y complementados para reforzar los procesos y políticas que son exigidos por la PCI DSS.

- Intercontact corre un gran riesgo al ejecutar actividades comerciales que involucran el tratamiento, almacenamiento y transferencia de datos del titular de la tarjeta en la campaña metlife, ya que en la actualidad cuenta con tan solo un 23 por ciento de controles de la PCI DSS en un estado definido, esto quiere decir que solo este porcentaje de controles está documentado, divulgado, pero no se realizan mediciones de su desempeño, con esto se puede decir que Intercontact en este momento podría acarrear multas o sanciones por ejecutar estas actividades sin el debido control.

- Es necesario capacitación o formación a los funcionarios y terceros de Intercontact para implementar la PCI DSS, ya que las funciones ejercidas en cargos como administradores de plataformas, dba's, desarrolladores, líderes de campañas, directores, entre otras van a cambiar y sus responsabilidades pueden ser más amplias. Con el fin de generar una implementación acorde de la PCI DSS, cada uno de los colaboradores deben tener claridad de cuáles son las nuevas responsabilidades y funciones que van ejercer a partir de la fecha.

- El cronograma propuesto está diseñado para ser ejecutado en un lapso de año y medio, en el cual se pretende que Intercontact logre cumplir con los controles estipulados por la PCI DSS, se debe tener en cuenta que a lo largo de este año y medio la norma puede ser actualizada y algunos controles pueden cambiar, también que las fechas se pueden extender por motivos de problemas de inversión en componentes tecnológicos, falta de personal que asuma roles o responsabilidades o que la implementación de un control tome más tiempo del planificado.

- Para implementar la PCI DSS es necesario tener presente el gran esfuerzo que se requiere de todas las áreas involucradas relacionadas con el entorno de los datos del titular, esto involucra compromiso, ampliación de funciones, ejecución de nuevos procesos y políticas por parte de los colaboradores y terceros. Tener en cuenta que la alta dirección debe involucrar dentro de su presupuesto anual la implementación de la PCI DSS, como se indicó a lo largo del documento para

la ejecución de varios controles se requerirá de tecnología o adquisiciones especiales que acarrean un gasto tanto para su implementación, administración y mantenimiento.

- Intercontact podrá gestionar y procesar de manera adecuada, segura y eficiente los datos de la tarjeta crédito, débito y datos del titular para la operación Metlife ejecutando y realizando todas las actividades involucradas en los diferentes planes de acción, recomendaciones y cronograma de actividades mostrados en el presente documento que esta ceñido en el cumplimiento de controles de la PCI DSS.

14. RECOMENDACIONES

- Para la implementación de la PCI DSS se debe considerar en el presupuesto anual de la compañía los gastos que se deben ser involucrados para dar cumplimiento a esta norma.

- Asignar un líder de proyecto que esté a cargo del cumplimiento de cada una de las áreas o procesos que deben ser implementados y que los tiempos de implementación y ejecución se cumplan como están planteados.

- Dar cumplimiento con los tiempos propuestos en el cronograma, para que la culminación de proyecto no supere año y medio y tal vez la versión vigente de PCI DSS del año 2019 no genere traumatismo en los cambios significativos que deben ser involucrados.

- La alta dirección de Intercontact debe generar los nuevos roles, perfiles y funciones que deben ser necesarios para la implementación y mantenimiento de la PCI-DSS. Deben existir compromisos en conjunto con Metlife para que ellos también se alinean a los cambios y mejores que involucra la implementación de este proyecto.

- Aprovechar de la mejor manera los procedimientos, políticas y actividades del sistema de gestión de seguridad de la información que pueden ser usados en la implementación de la PCI DSS, con el fin de no crear de cero procedimientos que a la fecha existen pero por falta madurez o alcance en su ejecución no cumplen con el control impuesto por PCI DSS.

- Establecer fechas de seguimiento en la implementación del proyecto para establecer acciones correctivas o planes de acción para dar cumplimiento en tiempos adecuados.

- Usar Herramientas libres o con licenciamiento GNU para dar cumplimiento a algunos controles de la PCI DSS y que ahorrarían gastos en la implementación de los mismos.

- En las formaciones realizadas por la compañía se deben involucrar los temas relacionados a la PCI DSS de la misma manera que se realiza formación en el

sistema de gestión de seguridad de la información con el fin que todos los funcionarios sean conscientes de que sus funciones o tareas involucran el cumplimiento de esta norma.

- Luego de implementar la PCI-DSS en la compañía realizar la autoevaluación utilizando un cuestionario provisto por el Consorcio del PCI (PCI SSC).

15. BIBLIOGRAFÍA

ACOSTA David. PCI Hispano. Contenido bajo Licencia Creative Commons Atribucion-CompartirIgual 3.0. Proyecto cooperativo en idioma español entre profesionales de América y Europa para compartir conocimiento y experiencias en el proceso de implementación de estándares del PCI SSC. 2016. Fecha de consulta: [10 de Abril de 2017]. Disponible en: http://www.pcihispano.com/

BAVOTA. Magazine Premium. All Rights Reserved. Todo lo que necesita saber sobre PCI (*Payment Card Industry Security Standards*). 2013. Fecha de consulta: [19 de Febrero de 2017].Disponible en: http://www.magazcitum.com.mx

CMMI (*Capability Maturity Model Integration*)- Guía para la Integración de Procesos y la Mejora de Productos-Pearson Education S.A Año 2009 Segunda Edición.

FIREWALL- How Traditional *Firewalls* Fail Todays Networks – And Why Next-Generation *Firewalls* Will Prevais

FIREWALL- PCI Security Standards Council, LLC. Normas de seguridad de datos de la PCI (industria de tarjetas de pago), versión 3.0 © 2006-2013 Todos los derechos reservados. Noviembre de 2013

HASH – NIST Special Publication 800-107

HASH- Jorge Ramió Aguirre. Libro Electrónico de Seguridad Informática y Criptografía, Universidad Politécnica de Madrid – España 1 de marzo de 2006; Sexta Edición Versión 4.1

HERNÁNDEZ MOLINA, Ignacio. La formulación de proyectos en ciencias e ingenierías. Primera edición. Universidad piloto de Colombia. Bogotá D.C. 2012.

HERNÁNDEZ SAMPIERI, Rober. Metodología de la investigación. Segunda edición. McGraw-Hill INTERAMERICANA EDITORES, S.A de C.V 1998, 1991. México D.F

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO 9564 Financial services — Personal Identification Number (PIN) management and security. 2011

INTERNET SECURITY AUDITORS, Implantación y certificación en el estándar PCI-DSS .L Santander, 101, E-08030 Barcelona. (España). 2016. Fecha de consulta: [7 de Abril de 2017]. Disponible en: http://www.isecauditors.com/consultoria-pa-dss

ISO/IEC 27005 De 2008 .Gestión de Riesgos de la Seguridad

ISO/IEC 7816 Token criptográfico_

NIST SPECIAL PUBLICATION 800-57-Criptografía sólida

NIST SPECIAL PUBLICATION 800-115 Technical Guide to Information Security Testing and Assessment.

PCI HISPANO. Criterios para escoger un Proveedor Aprobado de Escaneo (ASV). 2016. Disponible en: pcihispano.com

PCI SECURITY STANDARDS COUNCIL, LLC. Normas de seguridad de datos de la PCI (industria de tarjetas de pago), versión 3.0 © 2006-2013 Todos los derechos reservados. Noviembre de 2013

PCI SECURITY STANDARDS COUNCIL. Payment Card Industry PTS POI Security Requirements v4.0. PCI Security Standards Council LLC. Copyright 2013

TRUNCAMIENTO **-** Norma de seguridad de datos (DSS) de la Industria de tarjetas de pago (PCI) y Normas de seguridad de datos para las aplicaciones de pago (PA-DSS)